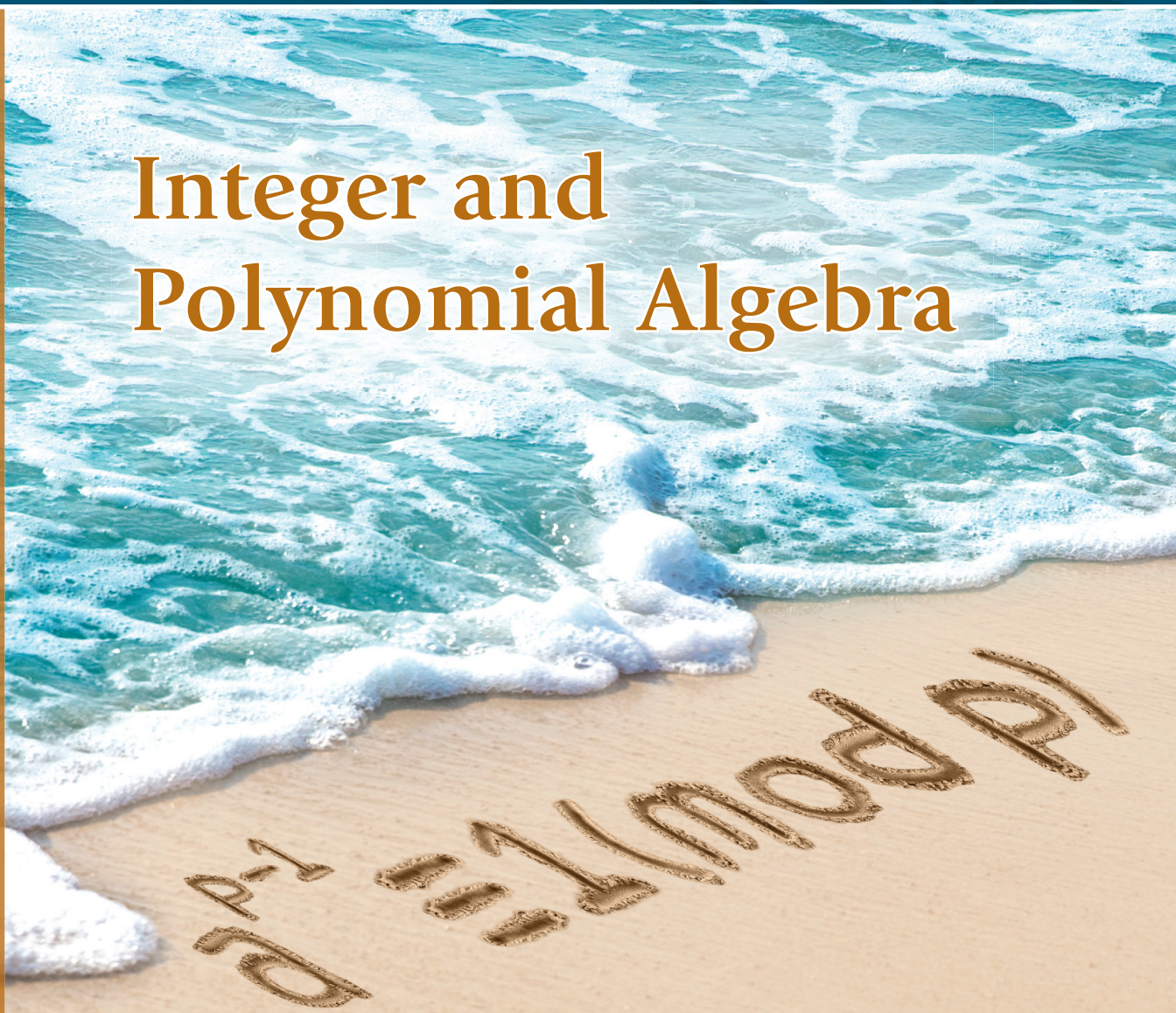
MATHEMATICAL WORLD VOLUME 31

Integer and Polynomial Algebra



Kenneth R. Davidson
Matthew Satriano

AMS American Mathematical Society

Integer and Polynomial Algebra

MATHEMATICAL WORLD VOLUME 31

Integer and Polynomial Algebra

Kenneth R. Davidson
Matthew Satriano

AMS AMERICAN MATHEMATICAL SOCIETY
Providence, Rhode Island

Cover design based on picture/iStock/Getty Images Plus
and MediaProduction/E+ via Getty Images.

2020 *Mathematics Subject Classification*. Primary 11-01, 12-01, 13-01.

For additional information and updates on this book, visit
www.ams.org/bookpages/mawrld-31

Library of Congress Cataloging-in-Publication Data

Cataloging-in-Publication Data has been applied for by the AMS.
See http://www.loc.gov/publish/cip/.
DOI: https://doi.org/10.1090/mawrld/31

---

10 9 8 7 6 5 4 3 2 1 28 27 26 25 24 23

Dedication

To Virginia, Colin, Stuart and Zoé.
–K.R.D.

To Waiwai and Quinn, and in loving memory of Susan Satriano.
–M.S.

Contents

Preface

This little book began as a set of course notes for an unusual but very attractive freshman course in algebra for math majors. The course introduces students to the notions of rigorous mathematics in the familiar settings of the integers and polynomials. This is worthwhile because of the strong parallels between the two theories. Indeed, one can argue that it is these parallels that led to the theory of commutative algebra as a unifying force.

The current book is an expanded version of those notes. Some material has been added, and many more exercises are included. Historical notes are given at the end of each chapter with references to a few sources for the material.

These topics have the advantage of being somewhat familiar to a good high school graduate, yet harbour many interesting unforeseen results. The number of different proof techniques in the book makes this a good introduction to a wide variety of new ideas. In particular, special emphasis has been paid to the role of algorithms in mathematics. Due to the increased use of symbolic computing, and especially because of the availability of MAPLE here at Waterloo, it has been natural to investigate the theory behind many of these computations. It also provides an opportunity to have student work out problems with much larger numbers. Many other symbolic computation programs, such as MATHEMATICA, are equally good for use in this course.

This course has been taught at the University of Waterloo for over thirty years. Until about a decade ago, roughly 800–1200 first year students in the mathematical sciences took a course using the textbook *Classical Algebra* by W.J. Gilbert, now in a revised edition [**13**] co-authored by S.A. Vanstone. About 5% of these students took the 'advanced' version using these notes.

These notes were used for a one semester course. We would cover much of the material in this book, but not all. In writing this book, it has seemed advisable to expand on certain connections beyond the scope of the course. It is hoped that this will provide greater flexibility for the instructor and additional reading for the interested student.

Students entering university to study mathematics have probably encountered prime numbers. Chances are great that they believe every integer factors uniquely into a product of primes, but have not seen a proof. This important fact, known as the Fundamental Theorem of Arithmetic, is of crucial importance in the theory of numbers. It is not easy to prove. More importantly, it is not *intuitively obvious*. Indeed, its significance is only realized with very large numbers beyond our real experience. The crucial fact that enables us to prove this with relative ease is the Euclidean Algorithm for finding greatest common divisors. Chapters 1 and 2 deal with these basic properties of the integers and modular arithmetic. After giving the proof of the Fundamental Theorem of Arithmetic, we show that, in fact, the proof technique applies in much greater generality. In Section 1.8, we define Euclidean Domains and prove that all such rings have unique factorization. Throughout the book, we see applications of this general theorem in a large variety of setting, such as the Gaussian integers and polynomial rings over a field.

It is worth noting that there are number systems not very much different from the integers in which unique factorization into primes fails. Far from being a disaster, this is an opportunity to investigate why this phenomena occurs. It shows us which properties of the integers themselves are crucial to make the theory work. That is why we make a foray into quadratic number domains in Chapter 3. Already the material covered in Chapters 1–3 allow us to prove Quadratic Reciprocity, one of the crowning achievements of elementary number theory.

A nice application of modular arithmetic is the Rivest-Shamir-Adelman public key cryptography scheme. This code, which is covered in Chapter 4, allows the author to publish the method of *encoding* a message in a public place, while keeping the method of *decoding* the message secret. This is a rather different idea in coding, as for all previously known codes, the method of decoding merely reversed the encoding method. The secret here is that it is very easy (with a computer) to find large primes (say 200–300 digits) but very difficult to factor the product of two large primes. When one first encounters the problem of determining if a given number is prime, it is natural to try the brute force method of dividing by all numbers up to the square root. However, it turns out there are beautiful and clever methods to test for primality without finding any factors at all. We delve more deeply into this subject, briefly discussing the Agrawal-Kayal-Saxena algorithm and its connection to the topics we have seen thus far. We also discuss the probabilistic test due to Miller-Rabin.

In Chapter 5, we introduce the complex numbers. There is a tacit assumption that the student is already reasonably familiar with the real numbers from studying calculus. However, a section is devoted to a brief discussion of how the real numbers are developed. The main result of this chapter is the Fundamental Theorem of Algebra, which states that every complex

polynomial factors into a product of linear terms. We emphasize how *analytic* techniques play a key role in the proof of this cornerstone *algebraic* result. The proof we give is one of the simplest, and relies on the Extreme Value Theorem. We also develop the complex exponential function, which plays a vital role in applications of the complex numbers.

In Chapter 6, we show that the same theory developed for the integers applies to the algebra of polynomials. In particular, there is a Euclidean Algorithm and unique factorization into irreducible polynomials. We examine various tests for irreducibility, and study connections with irrationality of the roots. We then follow up with special topics about real and complex polynomials such as Sturm's Theorem for counting real roots, and the formula for solving cubics. In Chapter 7, we study finite fields in some detail. We draw parallels between modular arithmetic for the integers and arithmetic modulo an irreducible polynomial. Many of the results we have seen for $\mathbb{Z}_p$ in earlier chapters carry over to all finite fields. A rather beautiful application of these ideas is an algorithm for factoring polynomials over the rationals. This algorithm is based on a method for factoring polynomials modulo a prime integer p. It turns out that factoring a polynomial of degree d mod p is much easier than factoring a d digit base p number.

We would like to take this opportunity to thank the people who have helped with this endeavour. In particular, the first author thanks Stanley Burris with whom he has had many enjoyable conversations about this material. The first author also thanks Keith Geddes for some conversations on the algorithms used by MAPLE. The second author would like to thank David Jao and Stephen New for answering questions about the practical aspects of RSA. It is a pleasure to thank Anton Mosunov for a careful reading of an early draft of the new version of this book and for sending us detailed comments and corrections. We thank the referees and editors at AMS/MAA for their helpful comments. Lastly, we thank the many students in Math 145 classes who suffered through various versions of these notes and offered many helpful suggestions and corrections.

Kenneth R. Davidson
Matthew Satriano
Waterloo, January, 2023

Chapter 1

The Integers

The basic object which we shall study in the first four chapters is the set of integers. As a mathematical object, the integers have a wealth of structure. First, you can add, substract and multiply integers together. It is the multiplicative structure which is of most interest, because the reciprocal operation of division is not always defined (within the integers). The notion of divisibility leads to the definition of prime numbers, and then to the factorization of numbers into primes. The reader may well have been told that every number factors into primes in a unique way. This non-trivial result is known as the Fundamental Theorem of Arithmetic. It is far from obvious. We will prove it in this chapter. In the last section, we will show that essentially the same argument will work in a very abstract context. The advantage of doing this is that we will later see several explicit, important contexts to which it applies, such as the ring of all polynomials.

1.1. Basic Properties

The integers is the set

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Beyond being a set, $\mathbb{Z}$ comes with the operations of addition and multiplication. Addition has an inverse operation called subtraction. However the inverse operation of multiplication, namely division, does not always yield an integer answer, which leads to the notion of divisibility. Describing the integers takes a little time, but the following list of properties is natural.

[S1] The **integers** consist of a set $\mathbb{Z}$ together with two binary operations **addition** $(+)$ and **multiplication** $(\cdot)$.

[A1] (**commutativity of addition**) For all $a, b \in \mathbb{Z}$,

$$a + b = b + a.$$

[A2] (**associativity of addition**) For all $a, b, c \in \mathbb{Z}$,

$$(a + b) + c = a + (b + c).$$

[A3] (**additive identity or zero**) There is an element $0 \in \mathbb{Z}$ so that for all $a \in \mathbb{Z}$,

$$a + 0 = a = 0 + a.$$

[A4] (**additive inverses**) For each $a \in \mathbb{Z}$, there is an element $-a \in \mathbb{Z}$ such that

$$a + (-a) = 0.$$

[M1] (**commutativity of multiplication**) For all $a, b \in \mathbb{Z}$,

$$a \cdot b = b \cdot a.$$

[M2] (**associativity of multiplication**) For all $a, b, c \in \mathbb{Z}$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

[M3] (**multiplicative identity or one**) There is an element $1 \in \mathbb{Z}$ so that for all $a \in \mathbb{Z}$,

$$a \cdot 1 = a = 1 \cdot a.$$

[D1] (**distributive law**) For all $a, b, c \in \mathbb{Z}$,

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

We did not define subtraction—it is enough to include the additive inverse. That is because $a - b$ is just an abbreviation for $a + (-b)$.

This is certainly a list of properties satisfied by the integers. But this collection of properties is satisfied by many other mathematical sets. For example, the collection $\mathbb{R}$ of all real numbers and $\mathbb{Q}$, the set of rational numbers (fractions). Also, the set

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\},$$

with the usual operations satisfies all these properties. Consider the set

$$\mathbb{Z} \oplus \mathbb{Z} = \{(a, b) : a, b \in \mathbb{Z}\}$$

with coordinate-wise addition and multiplication, i.e.,

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{and} \quad (a, b) \cdot (c, d) = (ac, bd).$$

This also satisfies these laws. What are the zero and one in this case?

In fact a great many mathematical objects satisfy these laws. They are called **commutative rings**. The word **ring** is used for a set satisfying all these laws except M1–commutativity of multiplication, and with another distributive law added:

[D2] For all $a, b, c \in \mathbb{Z}$,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

The set of 2×2 matrices with integer entries is an example of a non-commutative ring. Addition is coordinate-wise, but multiplication is defined by the rule

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{bmatrix}.$$

1.1.1. Example. Another important example that will play an important role in this book is the set of integers **modulo** n. For now, consider the ring $\mathbb{Z}_2$ consisting of two elements $\{0, 1\}$ with operations given by the tables:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Notice that in this example, unlike the others, $1 + 1 = 0$. This may seem rather strange, but it gives us a clue about how to add further properties to the above list to ensure that the integers are the only example.

One property that will ensure we do not get too big a set is a stipulation that

[G1] $\mathbb{Z}$ is **generated** by $\{0, 1\}$ as a ring.

This means that we start with 0 and 1, and form all the elements needed to provide the *minimal* collection satisfying all our properties. Since a ring is *closed* under the operations of addition and multiplication, we need all the numbers of the form 1, $1 + 1$, $1 + 1 + 1$, $1 + 1 + 1 + 1$,.... You should convince yourself that the distributive law ensures that this set is closed under multiplication, as well as addition. In order to satisfy [A4], additive inverses, we *may* have to add in -1, $-(1+1)$,.... You should now convince yourself that this collection is rich enough to satisfy all the properties. This includes checking that $(-1) + (-1) = -(1 + 1)$, etc. None of the necessary steps are hard, but it is very time-consuming to write them all out.

Unfortunately, this still does not ensure that we have the integers. The example $\mathbb{Z}_2$ above is also generated by its 0 and 1. We can eliminate this example by decreeing that 1, $1+1$, $1+1+1$, $1+1+1+1$,... are all different. If this holds in any ring, the collection $S = \{1,1+1,1+1+1,1+1+1+1,\ldots\}$ will be indistinguishable from the **natural numbers** $\mathbb{N} = \{1, 2, 3, \ldots\}$ by any mathematical property. In fact, to ensure that they are all different, it is enough that none are 0. Why? Then it follows that $-S$ does not intersect S (why?), and that $R = S \cup \{0\} \cup -S$ is a ring which has all the same properties as $\mathbb{Z}$. We will name this last property [F1] for free:

[F1] No nontrivial sum of 1's is equal to 0.

We have not written down all the important properties of the integers. But at least, we have come up with a list of properties that distinguishes the integers from other similar objects. Before leaving this point, we will show how we can define another very useful property – **order** – using what we already have. Define order as follows:

$$\begin{aligned} a < b &\quad \text{if} \quad b - a \in \mathbb{N} \\ a = b &\quad \text{if} \quad b - a = 0 \\ a > b &\quad \text{if} \quad b - a \in -\mathbb{N}. \end{aligned}$$

This order satisfies some simple properties:

[O1] For all a, b, and c in $\mathbb{Z}$ with $a < b$, $a + c < b + c$.
[O2] For all a, b, and c in $\mathbb{Z}$ with $a < b$ and $c > 0$, $ac < bc$.

We say that an integer n is **positive** if $n > 0$. Notice that by definition of the ordering on $\mathbb{Z}$, an integer n is positive if and only if $n \in \mathbb{N}$.

What do we mean when we say that two mathematical objects are the same? or at least have exactly the same properties? Throughout mathematics, one is concerned about this issue. It is generally dealt with by considering maps between sets that preserve the structure that one is studying. The following definition captures part of this for rings.

1.1.2. Definition. If R and S are rings, a function $\varphi\colon R \to S$ is called a **ring isomorphism** if

- φ is a bijection (i.e., one-to-one and onto) such that
- $\varphi(0) = 0$ and $\varphi(1) = 1$,
- $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ for all $r_1, r_2 \in R$,
- $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$ for all $r_1, r_2 \in R$.

Say R and S are **isomorphic** if there exists a ring isomorphism $\varphi\colon R \to S$.

If R and S are isomorphic rings, then they are indistinguishable on the basis of their properties as rings. We consider them to be equivalent objects. See Exercise 7. The new ring is just the integers 'in disguise'.

Exercises

1. Show that $\mathbb{Z}[\sqrt{3}]$ is a commutative ring.

2. Show that if $[F1]$ holds, then sums of different numbers of 1's are all distinct, and their additive inverses are all distinct from sums of 1's.

3. Verify the properties of a commutative ring for $\mathbb{Z}_2$.

4. Can an operation $<$ be put on $\mathbb{Z}_2$ satisfying [O1]?

5. Describe explicitly the ring $\mathbb{Z}[\sqrt[3]{5}]$ generated by 1 and $\sqrt[3]{5}$.

6. (a) What are the additive and multiplicative identities for $\mathbb{Z} \oplus \mathbb{Z}$?
(b) Show that there are non-zero elements in $\mathbb{Z} \oplus \mathbb{Z}$ which multiply to 0.

7. Consider the ring $R = \{2^n : n \in \mathbb{Z}\}$ with addition $\oplus$ given by $2^n \oplus 2^m = 2^{n+m}$, and multiplication $\odot$ given by $2^n \odot 2^m = 2^{nm}$. Show that this is a ring. Then show that the map taking 2^n to its logarithm base 2 (namely n) is a ring isomorphism from R to $\mathbb{Z}$.

8. What other properties of the integers can you think of? Can these properties be deduced from [S1], [A1]–[A4], [M1]–[M3], and [D1]?

1.2. Well Ordering Principle

In this section, we will look at a 'self evident' principle. We shall see that it leads us to the principle of induction, a basic proof technique which we will introduce here. In mathematics, one does have to be careful about what we think is self-evident, as this is not as clear as the reader might think. This principle can be justified.

1.2.1 Well Ordering Principle. *Every non-empty subset of* $\mathbb{N}$ *has a least element.*

This is true for the following reason. If S is a non-empty subset of $\mathbb{N}$, then it contains an element s. Consider the *finite* list of integers $1, 2, 3, \ldots, s$. The first integer in this list which belongs to S is the desired least element.

We will use this principle to formalize certain arguments. First, let us consider induction. Induction is a method used to verify a long (often infinite) list of propositions. Call the propositions $P(n)$ for $n \in \mathbb{N}$. That is, each $P(n)$ is a mathematical statement which might be true or false.

1.2.2 Principle of Induction. *Suppose that proposition* $P(1)$ *is true. Furthermore, suppose that if* $P(k)$ *is true for* $1 \leq k < n$*, then* $P(n)$ *is true. Then* $P(n)$ *is true for all* $n \geq 1$*.*

Proof. Let S be the set of all n such that $P(n)$ is false. If S is empty, we have the desired conclusion. Otherwise, S is non-empty. In this case, the Well Ordering Principle tells us that S has a least element, say n. By the hypotheses, $n \neq 1$. Since n is the smallest integer in S, we see that $P(k)$ is true for all $1 \leq k < n$. By the induction hypothesis, $P(n)$ is true. This contradicts the fact that $P(n)$ is false. The contradiction must be due to a false supposition – in this case, that must be the supposition that S is non-empty. So S is empty, and $P(n)$ is true for all $n \geq 1$. ■

Sometimes this is called the generalized principle of induction because it assumes that all of the statements $P(k)$ for $1 \leq k < n$ must be known to be true in order to deduce $P(n)$, not just $P(n-1)$. This is sometimes an important improvement. See the Second Proof of Theorem 1.3.3 in the next section.

1.2.3. Example. We look for a formula for the sum of the first n squares: $s_n = \sum_{i=1}^{n} i^2$. The first few terms are $1, 5, 14, 30, 55, 91$. While no obvious formula is apparent, the reader can check that $P(n) : s_n = \dfrac{n(n+1)(2n+1)}{6}$ is valid for $n = 1, 2, 3, 4, 5, 6$. We will use induction to verify this for all $n \geq 1$.

First

$$\frac{1(1+1)(2\cdot 1+1)}{6} = \frac{6}{6} = 1 = s_1.$$

Thus $P(1)$ is true. In this example, to check $P(n)$, it is enough to use the fact that $P(n-1)$ is true. Then

$$s_n = s_{n-1} + n^2 = \frac{(n-1)(n)(2n-1)}{6} + n^2 = \frac{2n^3 - 3n^2 + n + 6n^2}{6}$$
$$= \frac{2n^3 + 3n^2 + n}{6} = \frac{n(n+1)(2n+1)}{6}.$$

Thus if $P(n-1)$ is true, so is $P(n)$. By induction, this formula holds for all $n \geq 1$.

1.2.4. Example. Consider the following 'proof' by induction. We will show that all people have the same colour hair. Let $P(n)$ be the statement that every set of n people all have the same hair colour. This is evident for $n = 1$. Now look at larger n. Suppose that $P(n-1)$ is true. Given a group of n people, apply the induction hypothesis to all but the last person in the group. This group have all the same hair colour. Now repeat this argument with all but the first person. We find that all the people have the same hair colour by combining these two facts. By induction, all people have the same hair colour.

This is patently absurd, and you are undoubtedly ready to refute this by saying that Eric has different hair colour from Alana. But we want you to find the mistake in the induction argument.

Exercises

1. Prove by induction that

$$\sum_{i=1}^{n} i^3 = \Big(\sum_{i=1}^{n} i\Big)^2.$$

2. Prove by induction that

$$\sum_{i=1}^{n} (-1)^i i^2 = \frac{(-1)^n n(n+1)}{2}.$$

3. Find the error in the induction argument in Example 1.2.4.
HINT: $P(1)$ is true, and $P(73)$ implies $P(74)$.

4. Prove that $n! > 2^n > n^2$ for $n \geq 5$.

5. Prove that if $x > -1$ is a real number and $n \geq 1$, then $(1+x)^n \geq 1+nx$.

6. Let $x > 1$ be a real number such that $x + x^{-1}$ is an integer. Prove that $x^n + x^{-n}$ is an integer for all $n \geq 1$.
HINT: evaluate $(x + x^{-1})(x^n + x^{-n})$.

7. Consider the Fibonnaci sequence, given by $F(0) = F(1) = 1$, and for $n \geq 0$, $F(n+2) = F(n) + F(n+1)$. Let $\tau = (\sqrt{5}+1)/2$. Prove by induction that

$$F(n) = (\tau^{n+1} - (-1/\tau)^{n+1})/\sqrt{5}.$$

8. Define a sequence of real numbers by the rules

$$s_0 = 0 \quad \text{and} \quad s_{n+1} = \sqrt{3 + s_n} \text{ for } n \geq 0.$$

(a) Show by induction that $s_n < s_{n+1} < 3$ for all $n \geq 0$.
(b) The least upper bound principle (see chapter 5) shows that the sequence has a limit. Show that the limit should be $\sigma = \frac{1+\sqrt{13}}{2}$.
(c) Obtain a formula for $\sigma - s_{n+1}$ in terms of $\sigma - s_n$. Hence prove by induction that $0 < \sigma - s_n < 3/4^n$ for all $n \geq 0$.

9. A real number x has a decimal expansion $x = x_0.x_1x_2x_3\ldots$ where $x_0 \in \mathbb{Z}$ and $x_i \in \{0, 1, 2, \ldots, 9\}$ for $i \geq 1$. Say that this expansion is *eventually periodic* if there are positive integers d and N so that $x_{n+d} = x_n$ for all $n \geq N$. Prove that a real number with eventually periodic decimal expansion is rational.
HINT: consider $10^{N+d}x - 10^N x$.

10. Let $x = \frac{p}{q}$ be a rational number, with $q \geq 1$.
(a) Find $r_k \in \{0, 1, \ldots, q-1\}$ so that $10^k = a_k q + r_k$ for $k \geq 0$. Show that there are two integers $0 \leq k < l \leq q$ such that $r_k = r_l$; so $q|(10^l - 10^k)$. HINT: the *pigeonhole principle* states that if $q+1$ objects are placed in q boxes, at least one box has two or more objects in it.
(b) Show that if $0 \leq a < 10^d - 1$, then $\dfrac{a}{10^d - 1}$ has a periodic decimal expansion.
(c) Prove that x has an eventually periodic decimal expansion.
HINT: consider $(10^l - 10^k)x$.

1.3. Primes

We have noted that division is not a part of the axioms for the integers. There are two good reasons for this. The first is that a/b is not defined *as an integer* for all pairs of integers a and b with $b \neq 0$. Secondly, division is the inverse relation to multiplication in the same way that subtraction is the inverse of addition. Subtraction does not occur in the axioms either; but is shorthand for combining addition with the additive inverse. For these reasons, we define divisibility in terms of multiplication.

1.3.1. Definition. Say that an integer a **divides** an integer b if there is an integer c such that $b = ac$. The notation for this is $a|b$.

An integer p is **prime** if $p \neq \pm 1$ and the only integers which divide p are ± 1 and $\pm p$.

We don't consider ± 1 to be prime because they are invertible in $\mathbb{Z}$; and are called **units** of $\mathbb{Z}$. They divide every number, and this does not substantially change the factorization. Note that ± 2 and ± 3 are primes. So

$$6 = 2 \cdot 3 = (-2)(-3) = 3 \cdot 2 = (-3)(-2).$$

These are considered to be trivial differences because permutation of factors is irrelevant since multiplication is commutative, and -1 is a unit, so that we can put this as a factor into any term. Common practice is to factor positive integers into a product of positive primes in increasing order.

The most important fact about factoring integers is that each integer can be written as a product of primes in exactly one way (up to signs and permutation of the factors). This is known as the Fundamental Theorem of Arithmetic. It is not particularly easy to prove. Indeed, it would be quite an accomplishment to do this properly without having seen a proof yourself. We will prove this theorem in this book, but it will take some preparation.

In this section, we content ourselves with something easier—*existence* of a factorization into primes.

1.3.2. Lemma. *If $n = ab$ with $a, b \in \mathbb{N}$, then $a \leq n$. In particular, if $b \neq 1$, then $a < n$.*

Proof. Since $b \in \mathbb{N}$, we have $1 \leq b$. Thus, $a \leq ab = n$. Furthermore, if $b \neq 1$, then $1 < b$ and so $a < ab = n$. ■

1.3.3. Theorem. *Every integer $n > 1$ is the product of a finite set of primes.*

Proof. Let S be the set of all integers $n > 1$ which are **not** the product of finitely many primes. We want to prove that S is empty. If it is not empty, then by applying the Well Ordering Principle, we obtain a least integer n which cannot be factored into primes. If n were prime, it would be the product of *one* prime, namely itself. So, n cannot be prime and we may write $n = ab$ where a and b are positive integers, neither of which is 1. By Lemma 1.3.2, we see a and b are less than n, so they cannot belong to S. Therefore both can be factored into primes, say

$$a = p_1 p_2 \dots p_k \quad \text{and} \quad b = q_1 q_2 \dots q_l.$$

Then n can be factored as $n = p_1 p_2 \dots p_k q_1 q_2 \dots q_l$. This contradicts the fact that n is in S, and so S must be empty. ■

Second Proof. This is the same proof, but using induction rather than the Well Ordering Principle. Notice that we need the full generality of the Principle of Induction.

Let $P(n)$ for $n \geq 2$ be the statement that n factors as the product of primes. Check by hand that 2 is prime, and so $P(2)$ holds. See Exercise 5. (This is our starting point, since there is no statement $P(1)$.) Now suppose that $P(k)$ holds for all $k < n$. If n is prime, then it is the product of one prime, so $P(n)$ holds. On the other hand, if n is not prime, factor $n = ab$ for $a, b > 1$. As above, $1 < a, b < n$. By the induction hypothesis, $P(a)$ and $P(b)$ are true. (Here is where the full strength of the induction hypothesis is required.) Therefore, we can factor a and b into products of primes. As above, we can multiply them together to obtain a factorization of n into a product of primes. By induction, the theorem is true for all $n \geq 2$. ■

Why is this not enough for the Fundamental Theorem mentioned above? Because we do not know if the product of two different sets of primes can be the same! For small numbers, you know from experience that there is only one way to factor them. This property is known as **Unique Factorization**. But how many 1000 digit numbers have you tested? If the answer is more than one, what about numbers with $10^{10^{10}}$ digits? We need an argument that goes beyond this common experience. The tool we need is the Euclidean algorithm, which we develop in a later section.

Exercises

1. Let a, b, c, r, s be integers. Show that if $a|b$ and $a|c$, then $a|(br + cs)$.

2. Show that if $a|b$ and $b|c$, then $a|c$.

3. Show that if c and d are integers such that $c|d$ and $d|c$, then $d = \pm c$.

4. Show that if $1 < a \in \mathbb{N}$ has no divisor p with $1 < p \leq \sqrt{a}$, then a is prime.

5. Use Lemma 1.3.2 to show that 2 is prime.

6. Show that if a product of integers $a = a_1 a_2 \cdots a_n$ is even, then at least one of the factors a_i must be even.

7. Show that if a product of integers $a = a_1 a_2 \cdots a_n$ is a multiple of 3, then at least one of the factors a_i is a multiple of 3.

8. Does your method of proof in the previous question give any insight into what happens when we replace 3 by 1049?

9. **(Sieve of Eratosthenes)** Imagine that you have listed all of the integers from 1 to 10000. Cross out 1. Now 2 is the first remaining number. Cross out every second number following 2, i.e., $4, 6, 8, \ldots$. Now 3 is

the next remaining number. Cross out every third number following 3, i.e., $6, 9, 12, \ldots$. Some numbers like 6 and 12 are crossed out more than once. Show that after you have crossed out all multiples of 97, what remains is a list of all primes less than 10000.

1.4. Many Primes

In this section, we will give two proofs that there are infinitely many primes. The first proof of this fact is credited to Euclid, and dates from about 200 BCE (see Exercise 2). Our first proof is slightly easier. Our second proof is much harder, and you may skip it without loss. But it gives some indication that primes are quite plentiful, whereas with the first proof, primes could still be very rare.

In fact, the famous Prime Number Theorem shows that the number $\pi(n)$ of primes less than or equal to n is approximately $n/\log(n)$ in the sense that

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\log n} = 1.$$

Because the log function grows very slowly, this means that primes are quite common. The prime number theorem was conjectured by Legendre and Gauss about 200 years ago. They used extensive tables of primes to test the conjecture, but were not able to prove it. Riemann introduced the famous Riemann zeta function, and established important relationships between the properties of this function and the distribution of the primes. One of the most important outstanding mathematical problems, known as the "*Riemann hypothesis*", asks about the location of the zeros of this function. In 1896, Hadamard and de la Valleé Poussin finally proved the prime number theorem, independently of each other, by obtaining partial information about the zeros of the zeta function.

1.4.1. Theorem. *There are infinitely many primes.*

Proof. Let $n \geq 1$. By Theorem 1.3.3 , there is a prime, say p_n, which divides $n! + 1$. If $p_n \leq n$, then $p_n | n!$ as well, and hence it would divide $(n! + 1) - n! = 1$, which is absurd. Thus $p_n > n$. Therefore the set of prime numbers is unbounded, and thus is infinite. ■

One way to gauge the density of the primes is the following result which says that the sum of the reciprocals of the primes diverges. For a quickly growing series like the powers of 2, the sum of the reciprocals converges quickly. For the set of perfect squares, one verifies that the sum of the reciprocals converges by the integral test from calculus. In fact, even for a series like $n \log n (\log\log n)^2$, the sum of the reciprocals converges. So prime numbers occur more frequently in some sense. Indeed, this gives some credence to the prime number theorem.

1.4.2. Theorem.

$$\sum_{p \text{ prime}} \frac{1}{p} \quad \textit{diverges.}$$

Proof. Let us number the primes in increasing order as $p_1 < p_2 < \ldots$. Again the proof proceeds by obtaining a contradiction if $\sum_i \frac{1}{p_i} < \infty$. In this case, the 'tail' of the series is small. So we can choose an integer k so that

$$\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}.$$

Fix the large integer $N = 4^{k+1}$. We will count the set $\{1, 2, \ldots, N\}$ in a different way. The first step is to count the numbers from 1 to N which have a big prime factor p_i for $i > k$. There are at most N/p_i numbers in this range which are multiples of p_i. Adding this up over all $i > k$, we find that there are at most

$$n = \sum_{i>k} \frac{N}{p_i} < \frac{N}{2}$$

numbers in $\{1, \ldots, N\}$ which have any of these primes as a factor. (This is a rather crude estimate because any multiple of more than one large prime is counted more than once; and if $p_i > N$, there are no multiples at all.)

Now the remaining numbers all have the form

$$a = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}.$$

To count these, we factor out the biggest square possible. That is, we write $a = b^2 c$ where

$$b = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots p_k^{m_k} \quad \text{and} \quad c = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots p_k^{e_k},$$

where if $n_j = 2m_j$ is even, then $e_j = 0$ and if $n_j = 2m_j + 1$ is odd, then $e_j = 1$. There are at most $\sqrt{N}$ ways of choosing b since $1 \le b \le \sqrt{a} \le \sqrt{N}$. Since there are only two choices for each e_j, there are at most 2^k ways of choosing c. So altogether, there are at most $m = 2^k\sqrt{N}$ ways of obtaining numbers of this form in $\{1, \ldots, N\}$. (This estimate is crude too, but uses a trick that makes it pretty good.)

Combining these two estimates, we have counted all numbers from 1 to N at least once. So

$$4^{k+1} = N \le n + m < N/2 + 2^k\sqrt{N} = 2^{2k+1} + 2^k 2^{k+1} = 4^{k+1}.$$

This is an absurd statement, contradicting our hypothesis that the reciprocals of the primes converged. So the series must diverge. ■

Exercises

1. Show that there are arbitrarily long strings of consecutive composite numbers.

2. **(Euclid's proof)** Suppose that the list of primes is finite: $p_1, p_2, \ldots, p_n$. Consider a prime factor of $p_1 p_2 \cdots p_n + 1$. Conclude that there are infinitely many primes.

3. The Fermat numbers are the integers $F_n = 2^{2^n} + 1$.
(a) Show that $x + 1$ divides $x^{2s} - 1$ for any positive integer s. Hence show that F_n divides $F_m - 2$ for all $m > n$.
(b) Show that the F_n have no common prime factors. Hence give another proof that there are infinitely many primes.

4. Suppose that $p_1, \ldots, p_r$ is a list of distinct primes. Let $N = p_1 p_2 \ldots p_r$ and $q_i = N/p_i$. Define $M = \sum_{i=1}^{r} q_i$. Show that no p_i can divide M. Conclude that there are infinitely many primes.

5. Show that there are infinitely many primes of the form $4n + 3$.
HINT: for $n \geq 4$, show that $n! - 1$ has a prime factor p_n of this form.

6. Show that if $n > 1$ and $a^n - 1$ is prime, then $a = 2$ and n is prime.
HINT: factor the polynomial $x^n - 1$.

7.★ This is an exercise to see that the prime number theorem is plausible.
(a) Use the integral test to show that the following series converge:

$$\sum_{n=2}^{\infty} \frac{1}{n(\log n)^2} \quad \text{and} \quad \sum_{n=1}^{\infty} \frac{1}{n^2}$$

(b) Show that $\pi(n) > \frac{n}{(\log n)^2}$ infinitely often.
HINT: show that the sum of the reciprocals of the primes between 2^{k-1} and 2^k is at most $2^{1-k}\pi(2^k)$. Use this to estimate the sum of the reciprocals of all primes.

1.5. Euclidean Algorithm

Long division is an algorithm usually taught in elementary school that allows one to divide a (usually smaller) number into another (usually larger) one, and obtain an integer quotient and remainder. This is actually quite a strong result, as it is the key to establishing the Euclidean algorithm in the next section. Yet because it is familiar since childhood, we take it for granted. This is formalized as follows:

1.5.1 Division Algorithm. *Suppose $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then there are* ***unique*** *integers q and r such that*

$$b = aq + r \quad \textit{and} \quad 0 \leq r < a.$$

Proof. We will apply the Well Ordering Principle to the set of all positive remainders to obtain the smallest one. Let

$$S = \{s : s = b - aq \geq 0, \text{ and } q \in \mathbb{Z}\}.$$

First note that S is non-empty. For if $b \geq 0$, take $q = 0$ and obtain $b \in S$. And if $b < 0$, take $q = b$ to obtain

$$s = b - ab = b(1 - a) \geq 0.$$

Let r be the least element of S (whose existence is guaranteed by the Well Ordering Principle), and let q be the integer so that $r = b - aq$. If $r \geq a$,

$$s = b - (q + 1)a = r - a \geq 0$$

is a smaller element of S. Therefore $0 \leq r < a$.

It remains to verify uniqueness. Suppose that

$$b = aq_1 + r_1 = aq_2 + r_2 \quad \text{and} \quad 0 \leq r_i < a \quad \text{for } i = 1, 2.$$

Subtracting yields $a(q_1 - q_2) = r_2 - r_1$. But $-a < r_2 - r_1 < a$, so the only multiple of a in this range is 0. Hence $r_2 = r_1$, and thus $q_1 = q_2$. ■

1.5.2. Definition. The **greatest common divisor** of a pair of non-zero integers a and b is the largest number d, denoted $\gcd(a, b)$, which divides both of them. Two integers a and b are called **relatively prime** if $\gcd(a, b) = 1$.

The notion of largest common divisor, in terms of the natural order on $\mathbb{Z}$, is not directly compatible with divisibility. In other words, small numbers need not divide big ones. So one cannot say, without some additional argument, that the largest common divisor of two integers is related to other divisors in any multiplicative way. In fact, the reason that *all* divisors of two numbers divide the largest common divisor is the basis for proving that factoring numbers into primes is unique.

The theoretical and computational importance of the greatest common divisor lies in the fact that there is a simple algorithm for computing it, which, at the same time, reveals some of the deeper structure. This algorithm is known as the Euclidean algorithm. It is best seen through an example. But first, we describe the basic idea.

Start with two positive integers a and b, and say that $a > b$. Divide b into a to obtain a remainder r_1 and quotient q_1. From the division algorithm, we have $0 \leq r_1 < b$, and $r_1 = a - q_1 b$. Now divide r_1 into b to obtain a remainder r_2. Notice that r_2 can be expressed in terms of b and r_1, and hence in terms of a and b. Repeat this operation by now dividing r_2 into r_1, etc. Eventually, this process ends because the remainders are decreasing and must eventually reach zero. The last non-zero remainder will be the $\gcd(a, b)$. As we go along, we keep track of how to express all the remainders in terms of integer combinations of a and b.

1.5.3. Example. Consider the algorithm for $\gcd(901, 636)$. Now 636 goes into 901 $q_1 = 1$ times with remainder $r_1 = 265$. So $265 = 901(1) + 636(-1)$;

we write $s_1 = 1$ and $t_1 = -1$. Next 265 goes into 636 $q_2 = 2$ times with remainder $r_2 = 106$. Therefore,

$$\begin{aligned} 106 &= 636 - 265(2) \\ &= 636(1) - \big(901(1) + 636(-1)\big)(2) \\ &= 901(-2) + 636(3). \end{aligned}$$

We write $s_2 = -2$ and $t_2 = 3$. Repeating this procedure, we see that 106 goes into 265 $q_3 = 2$ times with remainder $r_3 = 53$. And

$$\begin{aligned} 53 &= 265 - 106(2) \\ &= \big(901(1) + 636(-1)\big) - \big(901(-2) + 636(3)\big)(2) \\ &= 901(5) + 636(-7). \end{aligned}$$

We set $s_3 = 5$ and $t_3 = -7$. Finally, 53 divides into 106 exactly 2 times with 0 remainder. The following chart helps to keeping track of this information.

r	q	s	t
901		1	0
636		0	1
265	1	1	-1
106	2	-2	3
53	2	5	-7
0	2	-12	17

Notice that one obtains the value of s and t in a given row by subtracting q times the row above from the row above that.

Now you should notice that 53 divides 901 and 636. The reason this happens is explained recursively. First, the fact that the next remainder is 0 means that 53 exactly divides 106. The equation $265 = 106(2) + 53$ shows that 53 divides 265. Next, one has $636 = (2)265 + 106$, so that 53 divides 636. Finally, since $901 = 636 + 265$, it is also a multiple of 53. Thus 53 is a common divisor of 636 and 901.

Next, suppose that d divides both 636 and 901. Then the equation $53 = 901(5) - 636(7)$ implies that d divides 53. In particular, 53 must be the biggest divisor because all common divisors of 636 and 901 divide it.

It seems worthwhile to try to set down the main ideas of the proof here in general. However, if you do not think that you already have the basic idea of how it goes, stop now and work out a couple of examples on your own. Then look over the example above again to see if the arguments make more sense. Experience shows that trying to understand the general argument before understanding the concrete example is often futile.

1.5.4 Euclidean Algorithm. *Given two positive integers $a > b$, use the division algorithm repeatedly to obtain a sequence of remainders r_i for*

$1 \leq i \leq k+1$ *until the last remainder* $r_{k+1} = 0$. *Then* $\gcd(a, b) = r_k$, *and there are integers* s *and* t *so that* $\gcd(a, b) = as+bt$. *Moreover, every divisor of both* a *and* b *divides* $\gcd(a, b)$.

Proof. For convenience of notation, we will write $r_{-1} = a$ and $r_0 = b$. Notice that a and b are combinations of themselves. That is, $a = a(1)+b(0)$ and $b = a(0) + b(1)$. So we define $s_{-1} = 1$, $t_{-1} = 0$, $s_0 = 0$, and $t_0 = 1$. Now we proceed with our algorithm by induction. At each stage, we have each remainder $r_i = as_i + bt_i$. If $r_i \neq 0$, divide it into r_{i-1} to obtain $r_{i-1} = r_i q_{i+1} + r_{i+1}$ with remainder $0 \leq r_{i+1} < r_i$. We have the equation

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_{i+1} \\ &= \big(as_{i-1} + bt_{i-1}\big) - \big(as_i + bt_i\big)q_{i+1} \\ &= a\big(s_{i-1} - s_i q_{i+1}\big) + b\big(t_{i-1} - t_i q_{i+1}\big). \end{aligned}$$

This writes r_{i+1} in the form $as_{i+1} + bt_{i+1}$, and in fact yields the *explicit expressions* $s_{i+1} = s_{i-1} - s_i q_{i+1}$ and $t_{i+1} = t_{i-1} - t_i q_{i+1}$. Since r_i is a strictly decreasing sequence of non-negative integers, this process eventually stops with a zero remainder r_{k+1}.

Now we work our way back up the list, proving that r_k divides all of the r_i. To begin, r_k divides itself; and the identity $r_{k-1} = r_k q_{k+1}$ shows that r_k divides r_{k-1}. Suppose that we have shown that r_k divides r_{i+1} and r_i. The identity $r_{i-1} = r_i q_{i+1} + r_{i+1}$ holds. Since r_k divides the right hand side of the equation, it must also divide r_{i-1}. Continue this process until it is shown that r_k divides both $r_0 = b$ and $r_{-1} = a$.

Lastly, it must be shown that every divisor d of both a and b divides r_k. Now $r_k = as_k + bt_k$. It is clear that d divides the right-hand side, hence d divides r_k. Thus $r_k = \gcd(a, b)$. ■

Extending 1.5.4 slightly further, we can give an alternative characterization of the gcd: while the gcd is defined to be the *greatest* common divisor, it turns out that it is also the *least* positive solution to a certain Diophantine equation. A **Diophantine equation** in an equation with integer coefficients for which we seek only integer solutions. This will be explored in greater depth in Chapter 3.

1.5.5. Corollary. *Let* a *and* b *be positive integers. Then* $\gcd(a, b)$ *is the least positive integer* d *for which there exist* $x, y \in \mathbb{Z}$ *with*

$$ax + by = d.$$

Proof. Let $d' = \gcd(a, b)$ and let d be the least positive integer for which the equation $ax + by = d$ has integer solutions. The Euclidean Algorithm 1.5.4 shows that there exist $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = d'$. Therefore, $d \leq d'$. On the other hand, $d' \mid a$ and $d' \mid b$, so we see d' divides $ax + by = d$, and hence $d' \leq d$. Therefore, $d' = d$. ■

Exercises

1. Prove that the remainder on division by 9 is obtained by the "casting out nines" algorithm. The method is to add the decimal digits of the given number. If the total is more than 9, repeat the procedure until the sum is a single digit. Replace 9 by 0. This result is the remainder after dividing by 9. Explain.

2. Find the gcd of each of the following pairs of numbers, and express it as an integer combination of these numbers.
(a) 31463 and 9782.
(b) 65778 and 52507.
(c) 5564737 and 5574221.
(d) 2452548 and 2943234.

3. Define $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$.
(a) Show that $\operatorname{lcm}(a, b)$ is a multiple of a and a multiple of b.
(b) Show that if $a|n$ and $b|n$, then $\operatorname{lcm}(a, b)|n$.

4. Prove the following formulae for integers a, b, d and k.
(a) $\gcd(a, b + ka) = \gcd(a, b)$.
(b) $\gcd(ka, kb) = |k| \gcd(a, b)$.
(c) $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ when $d = \gcd(a, b)$.

5. Write a computer program to implement the Euclidean algorithm. The input is $a, b \in \mathbb{N}$. The output should be $\gcd(a, b)$ together with $s, t \in \mathbb{Z}$ so that $\gcd(a, b) = as + bt$.

6. The last step of the Euclidean algorithm yields $0 = as_{k+1} + bt_{k+1}$. Show that $s_{k+1} = \pm b/d$ and $t_{k+1} = \mp a/d$, where $d = \gcd(a, b)$.
HINT: use induction to show that $s_i t_{i-1} - s_{i-1} t_i = \pm 1$.

7.★ Find all strictly increasing functions $f : \mathbb{N} \to \mathbb{N}$ such that $f(2) = 2$, and whenever $\gcd(m, n) = 1$, then $f(mn) = f(m)f(n)$.

1.6. Factoring Integers

In this section, we will prove the **Fundamental Theorem of Arithmetic**. This simply states that every number factors into primes in exactly one way. This is very important, and without the aid of the Euclidean algorithm, it would be very difficult to prove. In fact, we will see in section 3.3 that there are number systems which do not have this unique factorization property while others much like them do. So unique factorization is a special property which relies on important structural properties of the integers which are not immediately obvious.

The key to the proof is the following lemma, which follows quickly from the tools we have now. Try to prove it without the Euclidean algorithm.

1.6.1. Lemma. *If* $\gcd(a, b) = 1$ *and* $a|bc$*, then* $a|c$*.*

Proof. From the Euclidean algorithm, we obtain integers s and t such that $as + bt = 1$. Since $a|bc$, there is an integer d so that $ad = bc$. Thus,

$$c = (as + bt)c = a(sc + dt).$$

Therefore c is a multiple of a. ■

1.6.2. Corollary. *Suppose that a prime* p *divides the product* $a_1 a_2 \dots a_k$*. Then there is an index* j *so that* $p|a_j$*.*

Proof. We proceed by induction on k. This is evident for $k = 1$. For $k = 2$, this will follow from the lemma. For $\gcd(p, a_1)$ divides p, and thus is 1 or p. In the first case, the lemma yields $p|a_2$; while the latter yields $p|a_1$.

Now suppose that we have verified the result for $k - 1$. By hypothesis,

$$p|(a_1 \dots a_{k-1})a_k.$$

Applying the result for $k = 2$, we obtain $p|a_k$ or $p|a_1 \dots a_{k-1}$. If it is this second case, the induction hypothesis provides the desired conclusion. ■

Note that this is not the most basic type of induction. As well as needing the result for $k - 1$, we also need the $k = 2$ result. The following corollary is an immediate consequence of the one above, so no proof is needed. Make sure that you understand why this is the case.

1.6.3. Corollary. *If a prime* p *divides* a^k*, then* $p|a$*.*

The numbers ± 1 are **units** of $\mathbb{Z}$, meaning that they are invertible elements; namely $1 \cdot 1 = 1 = (-1)(-1)$. Any factorization into primes can be modified by multiplying each prime by a unit, provided that the product of all of the units used is 1. By convention, we consider a unit to be a product of no primes.

1.6.4 Fundamental Theorem of Arithmetic. *Every non-zero integer factors uniquely as a product of primes. More precisely, suppose* $n \geq 2$ *is an integer, and two factorizations into products of positive primes*

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

are given. If the factors are arranged so that $p_1 \leq p_2 \leq \dots \leq p_r$ *and* $q_1 \leq q_2 \leq \dots \leq q_s$*, then* $r = s$ *and* $p_i = q_i$ *for* $1 \leq i \leq r$*.*

Proof. Let us prove this by induction on n. Let $P(n)$ be the statement that n factors uniquely into a product of positive primes in increasing order. First suppose $n = 2$. We know that 2 is prime, and thus has a unique factorization $2 = 2$ as a product of primes; hence $P(2)$ holds.

Next suppose that the result holds for all $2 \leq m < n$. Furthermore, there is no harm in assuming that we listed our two factorizations of n so that $p_1 \leq q_1$. Since

$$p_1 | n = q_1 \dots q_s,$$

Corollary 1.6.2 above implies that p_1 divides some q_j. Since q_j is prime, this means $p_1 = q_j$. However $p_1 \leq q_1 \leq q_j = p_1$, so we see that $p_1 = q_1$. Let $m = n/p_1$. Then

$$p_2 \dots p_r = m = q_2 \dots q_s.$$

If $m = 1$, then $p_2 \dots p_r = 1$ which implies that $p_2 \dots p_r$ is the empty product, i.e. $r = 1$; and similarly $s = 1$. Therefore, $p_1 = n = q_1$ and the result is proven. If $m > 1$, then since $m < n$, by induction, $r-1 = s-1$ and $p_i = q_i$ for $2 \leq i \leq r$. Hence the result is also established for n. ■

Exercises

1. Factor into primes the number

$$n = (5564737)(5541307) = (5574221)(5531879).$$

You may assume that n has no factors less than 50.

2. Find $\gcd(100!, 3^{100})$. Why was this question not in the previous section?

3. How many terminal zeros are there in the decimal number 250!.

4. (a) Count the number of positive integer divisors of a number n with prime factorization $n = p^2q^6$ where p and q are distinct primes.
(b) Find a general formula for the number of divisors of p^aq^b.

5. Show that $\gcd(a^3, b^3) = \gcd(a, b)^3$.

6. A number is called *perfect* if it is equal to the sum of all of its proper positive integer divisors. For example, $6 = 1 + 2 + 3$. Show that if p and $2^p - 1$ are both prime, then $2^{p-1}(2^p - 1)$ is a perfect number.

7. If you have a symbolic manipulation program, factor n given that it is the product of

46090688629780653423712130445123786363894579014950692080 81

and

46090688629780653423712130538812156734263534632593387982 51

and is also the product of

46090688629780653423712130507582699944140549426712489308 13

and

46090688629780653423712130476353243154017564220831590712 87.

HINT: factoring such large numbers is slow, but gcd's are fast.

8. Let the set of all primes be listed in order as $p_1, p_2, p_3, \ldots$. Suppose that $n = p_1^{a_1} \ldots p_k^{a_k}$ and $m = p_1^{b_1} \ldots p_k^{b_k}$, where the superscripts a_i and b_i may be 0. Find the formula for $\gcd(n, m)$.

9. Suppose that p and q are consecutive odd primes. Prove that $p + q$ has at least three prime factors (not necessarily distinct).

10. Suppose that $a, b, c, d \in \mathbb{N}$ and $\gcd(a, b) = 1$. Show that if $ab = c^d$, then a and b are both dth powers.

11. Suppose that $a, b, c \in \mathbb{N}$ and $\gcd(a, b) = 1$. Show that if $c|ab$, then there is a unique factorization $c = c_1 c_2$ in $\mathbb{N}$ such that $c_1|a$ and $c_2|b$.

1.7. Irrational Numbers

An **irrational number** is a real number which cannot be expressed as a quotient of two integers. This may seem to be unrelated to the subject just covered. But in fact, many of the proofs of irrationality depend on unique factorization.

Let us look at the argument that $\sqrt{3}$ is irrational. It is proved by assuming that $\sqrt{3} = \frac{a}{b}$, where a and b are integers, and obtaining a contradiction. We may suppose that $\gcd(a, b) = 1$. Squaring and cross multiplying yields

$$3b^2 = a^2.$$

So 3 divides a^2, and hence by Corollary 1.6.3, 3 divides a. If we write $a = 3c$ and substitute into our equation, we obtain

$$3b^2 = 9c^2 \quad \text{and hence} \quad b^2 = 3c^2.$$

Repeating the argument, we see that 3 divides b. But then 3 divides $\gcd(a, b)$. This is absurd, and therefore $\sqrt{3}$ must be irrational.

There is some controversy about who first proved the irrationality of certain numbers. It was the school of Pythagoras who first showed that $\sqrt{2}$ was irrational. A number a is called **square free** if there is no integer $b > 1$ such that $b^2|a$. Plato credits his teacher Theodorus with the irrationality of the square roots of the square free numbers from 3 to 17. Scholars speculate that the reason for stopping at 17 is because the Fundamental Theorem of Arithmetic was not known. See [**15**, pp. 50–51.] We will see in Proposition 1.7.1 that these proofs hold in much more generality. Indeed, later in the section on polynomials, even stronger irrationality results can be obtained.

Here is a generalization of this fact.

1.7.1. Proposition. *Suppose that n and k are positive integers such that $\sqrt[k]{n}$ is rational. Then $\sqrt[k]{n}$ is an integer.*

Proof. Again let us write $\sqrt[k]{n} = \frac{a}{b}$ with $\gcd(a, b) = 1$. Taking the k-th power and cross multiplying, we obtain

$$nb^k = a^k.$$

If $b \neq 1$, let p be any prime factor of b. Then p divides a^k, and hence divides a. Therefore, p divides $\gcd(a, b)$. Since $\gcd(a, b) = 1$, b cannot have any prime factors; that is, $b = 1$. Hence $\sqrt[k]{n} = a$ is an integer. ■

Ad hoc methods can be used to prove that various *algebraic* expressions are irrational. (See the exercises) Later in this book, there will be more sophisticated ways of proving irrationality. For other important numbers such as π and e, one needs an *analytic* expression that defines these numbers in order to prove irrationality. It is much more difficult to show that these numbers do not satisfy any algebraic equation at all. Such numbers are called **transcendental**. It is possible to give an elementary proof of the irrationality of e. In chapter 6 we will give a much more devious proof that e is indeed transcendental.

1.7.2. Proposition. *e is irrational.*

Proof. We need an expression for e. A useful expression from calculus is

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}.$$

Suppose that $e = a/k$ where a and k are positive integers. Compute

$$a(k-1)! = k!e = \sum_{n=0}^{k} \frac{k!}{n!} + \sum_{n \geq k+1} \frac{k!}{n!}.$$

The first sum on the RHS is an integer. Hence there is an integer

$$a(k-1)! - \sum_{n=0}^{k} \frac{k!}{n!} = \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + \dots.$$

Estimate the size of this 'integer', say b, by summing a geometric series:

$$0 < b < \sum_{m=1}^{\infty} (k+1)^{-m} = \frac{(k+1)^{-1}}{1-(k+1)^{-1}} = \frac{1}{k} \leq 1.$$

There are no integers in this range, and so we have a contradiction. Hence e must be irrational. ■

Exercises

1. Show that $\beta := \sqrt{2}+\sqrt{3}$ is irrational. HINT: if $\beta = \frac{p}{q}$ with $\gcd(p,q) = 1$, do algebraic manipulations to eliminate the square roots, and deduce that $q|p$.

2. Show that $\gamma = \sqrt{2} + \sqrt[3]{5}$ is irrational.
HINT: if $\gamma = \frac{p}{q}$ with $\gcd(p,q) = 1$, get rid of the cube root first; then eliminate the square root.

3. Show that $\log_{10} 7$ is irrational.

4. Let $a_n \in \{1, 2, \ldots, 9\}$ for $n \geq 1$. Show that $\sum_{n\geq 1} \frac{a_n}{10^{n!}}$ is irrational.

5. Let α be a root of a polynomial $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, where $c_i \in \mathbb{Z}$ and $c_0 \neq 0$. Show that α is either an integer or is irrational. HINT: if $\alpha = \frac{a}{b}$ with $\gcd(a,b) = 1$, compute $b^n p(\alpha)$ in two ways, and deduce that $b|a^n$.

6. Find a monic polynomial with integer coefficients with $\sqrt{2} + \sqrt{3}$ as a root.

7. Find a monic polynomial with integer coefficients with $\sqrt{2} + \sqrt[3]{5}$ as a root.

8. Show that if k is not a power of any other integer, then $\log_k a$ is either an integer or irrational for each positive integer a.

9. In this exercise we show there exist irrational numbers q and r such that q^r is rational. Prove that one may take $r = \sqrt{2}$ with either $q = \sqrt{2}$ or $q = \sqrt{2}^{\sqrt{2}}$.

1.8. Unique Factorization in More General Rings

This section has a much greater level of abstraction than the rest of this chapter. It could be put off until a later point. However since the proof is fresh in our minds, it makes sense to do it here. Otherwise we will find ourselves providing the same proof repeatedly in various contexts.

Having now proved the Fundamental Theorem of Arithmetic 1.6.4, it is worthwhile to figure out the level of generality in which our proof is valid. You will notice that the Fundamental Theorem of Arithmetic relied on Euclid's algorithm 1.5.4, which in turn relied on the Division algorithm 1.5.1. We will see that any ring where an appropriate analogue of the division algorithm holds will satisfy a type of Euclidean algorithm. This will then be used to prove a version of the Fundamental Theorem of Arithmetic for any such ring.

To begin, a basic property that $\mathbb{Z}$ enjoys is that two non-zero integers cannot multiply to be zero. We are interested in rings in general that satisfy this constraint.

1.8.1. Definition. An element a of a ring R is a **zero divisor** if $a \neq 0$ and there exists a non-zero element $b \in R$ with $ab = 0$. A commutative ring R with no zero divisors is called an **integral domain**.

As we show in the next result, integral domains satisfy a familiar *cancellation property*. You will notice that this cancellation property for $\mathbb{Z}$ is used throughout the last few sections. So, in order to make the proof of the Fundamental Theorem of Arithmetic work in greater generality, it is important that we restrict attention to integral domains.

1.8.2. Lemma. *Let R be an integral domain. If $a, b, c \in R$ and $ab = ac$, then $a = 0$ or $b = c$.*

Proof. We see $a(b - c) = 0$ and since R has no zero divisors, we must have $a = 0$ or $b - c = 0$. ■

Since our ultimate goal in this section is to prove an analogue of the Fundamental Theorem of Arithmetic, we need a suitable notion of units and prime numbers. In general rings, primes are called irreducibles.

1.8.3. Definition. A **unit** of a ring R is an element x which has a multiplicative inverse y, i.e. there is an element y satisfying $xy = yx = 1$. We often write $y = x^{-1}$. The set of units of R is denoted by R^*.

1.8.4. Remark. In Exercise 5 you will prove that the y in Definition 1.8.3 is uniquely determined. Thus, the notation x^{-1} is unambiguous.

1.8.5. Example. In $\mathbb{Z}$, the units are ± 1. In $\mathbb{Q}$, every non-zero element is a unit. See Exercise 2 for some information on the units of $\mathbb{Z}[\sqrt{2}]$.

1.8.6. Definition. Let R be an integral domain. An element $p \in R$ is **irreducible** if $p \notin R^*$ and whenever $p = ab$ for $a, b \in R$, either a or b is a unit.

We next axiomatize what it means for a ring to have a division algorithm. The key property of the division algorithm 1.5.1 is that when we divide b into a, the absolute value of the remainder r is smaller than that of b. We will be interested in rings which, unlike $\mathbb{Z}$, may not have a useful ordering. (See Exercise 9.) Thus, we cannot literally require in our division algorithm

that $r < b$. However, we can look for an auxiliary function f which measures "how big" an element is and we can require that $f(r) < f(b)$.

1.8.7. Definition. An integral domain R is a **Euclidean domain** if there is a **Euclidean function** $f\colon R \to \mathbb{N}_0$ satisfying the following properties:

(1) $f(a) \leq f(ab)$ for all $a, b \in R$ with $b \neq 0$. (*order*)
(2) for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with

$$a = bq + r$$

and $f(r) < f(b)$. (*division*)

When we wish to emphasize the function f, we will say that (R, f) is a Euclidean domain.

1.8.8. Lemma. *Let (R, f) be a Euclidean domain. Then*

(1) *if $a \in R \setminus \{0\}$, then $f(0) < f(1) \leq f(a)$.*
(2) *if $a, b \in R \setminus \{0\}$, then $f(a) = f(ab)$ if and only if $b \in R^*$.*
(3) *if $b \in R \setminus \{0\}$, then $f(b) = f(1)$ if and only if b is a unit.*

Proof. If $a \neq 0$, then by the order property,

$$f(1) \leq f(1 \cdot a) = f(a).$$

Now take $a = b = 1$ and use the division property to write $1 = 1 \cdot q + r$ with $f(r) < f(1)$. This must mean that $r = 0$ and $f(0) < f(1)$. So (1) holds.

If $b \in R^*$, then $a = (ab)b^{-1}$, and so $f(ab) \leq f(a) \leq f(ab)$; whence $f(a) = f(ab)$. Conversely, suppose $f(ab) = f(a)$. By the division property, there exist $q, r \in R$ such that $a = (ab)q + r$ with $f(r) < f(ab) = f(a)$. Hence $r = a(1 - bq)$. If $r \neq 0$, we would get $f(a) \leq f(r) < f(a)$, a contradiction. So, we must have $0 = r = a(1 - bq)$. Since $a \neq 0$, Lemma 1.8.2 implies that $1 - bq = 0$. Thus $b \in R^*$. So (2) holds.

The third statement now follows by taking $a = 1$ in (2). ■

1.8.9. Remarks. In Exercise 6, you will show that if R has a function f satisfying the division property, then R has a Euclidean function.

In Exercise 8, you will show that if f is a Euclidean function and $g : \operatorname{Ran} f \to \mathbb{N}_0$ is strictly increasing, then $g \circ f$ is also a Euclidean function. Thus there are are many different choices for the Euclidean function; so this function is not unique. It means that we can always choose g so that $g(f(0)) = 0$ and $g(f(1)) = 1$. Thus we may suppose that $f(0) = 0$ and $f(b) = 1$ if and only if b is a unit.

1.8.10. Example. The integers $\mathbb{Z}$ is a Euclidean domain, where we take $f(n) := |n|$. Notice that this particular choice of f has a lot of structure: for example, $|ab| = |a|\,|b|$. Also if $a \mid b$, then $|a| \leq |b|$ and we have equality if and only if $a = \pm b$.

We will see many other examples of Euclidean domains throughout the course, such as the Gaussian integers (Section 3.5), other quadratic number domains (see Section 3.3 and Exercise 3 of Section 3.5), and polynomial rings over a field (Section 6.2). In this last example, the function f is the degree of the polynomial.

1.8.11. Example. We will show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain for the function $f(x) = |N(x)|$, where N is the norm function defined in Exercise 1. That is, if $x = x_1 + x_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, then $N(x) = x_1^2 - 2x_2^2$. Exercise 1 shows that f is multiplicative. Since f maps $\mathbb{Z}[\sqrt{2}]$ into $\mathbb{N}_0$,

$$f(ab) = f(a)f(b) \geq f(a) \quad \text{for all} \quad a, b \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}.$$

Suppose that $a = a_1 + a_2\sqrt{2}$ and $b = b_1 + b_2\sqrt{2} \neq 0$ are given. Let

$$\begin{aligned} x = \frac{a}{b} &= \frac{a_1 + a_2\sqrt{2}}{b_1 + b_2\sqrt{2}} \ \frac{b_1 - b_2\sqrt{2}}{b_1 - b_2\sqrt{2}} \\ &= \frac{a_1b_1 + 2a_2b_2}{N(b)} + \frac{a_1b_2 + a_2b_1}{N(b)}\sqrt{2} \\ &=: x_1 + x_2\sqrt{2} \in \mathbb{Q}[\sqrt{2}]. \end{aligned}$$

That is, x_1 and x_2 are rational. Choose integers c_1, c_2 so that $|x_1 - c_1| \leq \frac{1}{2}$ and $|x_2 - c_2| \leq \frac{1}{2}$. Define $c = c_1 + c_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then let

$$r = r_1 + r_2\sqrt{2} = a - bc = b(x - c) = b\big((x_1 - c_1) + (x_2 - c_2)\sqrt{2}\big).$$

Note that $r \in \mathbb{Z}[\sqrt{2}]$. However the norm is defined on $\mathbb{Q}[\sqrt{2}]$ and is multiplicative by Exercise 1. It follows that

$$N(r) = N(b)\big((x_1 - c_1)^2 - 2(x_2 - c_2)^2\big).$$

Now $(x_1 - c_1)^2 \in [0, \frac{1}{4}]$ and $(x_2 - c_2)^2 \in [0, \frac{1}{4}]$, so that

$$\big((x_1 - c_1)^2 - 2(x_2 - c_2)^2\big) \in \big[-\tfrac{1}{2}, \tfrac{1}{4}\big].$$

Therefore $f(r) = |N(r)| \leq \frac{1}{2}|N(b)| = \frac{1}{2}f(b)$. Thus $\mathbb{Z}[\sqrt{2}]$ has a division algorithm, and f is a Euclidean function.

Our next result shows that Euclidean domains satisfy a type of Euclidean algorithm. Since R is not necessarily ordered, we cannot speak of the greatest common divisor of a and b. However, the properties of r_k listed in theorem below capture the fact that r_k behaves like the gcd of a and b. Indeed, the first property says r_k is a common divisor of a and b; and the third property says that if e is any other common divisor, r_k must be "greater than" e in the sense that e divides r_k. Notice that in the case when $R = \mathbb{Z}$, this reduces to saying that $r_k = \pm\gcd(a, b)$.

1.8.12 Euclidean Algorithm for Euclidean Domains. *Let (R, f) be a Euclidean domain and $a, b \in R$ with $b \neq 0$. Then using the division algorithm repeatedly yields a sequence*

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_2 + r_3 \\ &\vdots \\ r_{k-1} &= r_kq_k + r_{k+1} \end{aligned}$$

with $r_1, r_2, \ldots, r_k$ non-zero, $r_{k+1} = 0$, and $f(b) > f(r_1) > \cdots > f(r_k)$. Furthermore, r_k satisfies the following properties:

(1) *$r_k \mid a$ and $r_k \mid b$,*
(2) *there exist $s, t \in R$ such that $as + bt = r_k$.*
(3) *for any $e \in R$, if $e \mid a$ and $e \mid b$, then $e \mid r_k$,*

Proof. For notational convenience, we let $r_{-1} = a$ and $r_0 = b$. Let us first show that the process terminates; i.e. there exists k with $r_{k+1} = 0$. Otherwise the process would define $r_i \neq 0$ for all $i \geq 1$. Consider the set

$$\{f(r_i) : r_i \neq 0,\ i \geq 1\}$$

with the r_i defined as in the statement of the theorem. Since all $f(r_i)$ are positive integers, by the well-ordering principle, there must be a least element $f(r_k)$. If $r_{k+1} \neq 0$, then we would have $f(r_{k+1}) < f(r_k)$ contradicting the fact that $f(r_k)$ is minimal. Thus, $r_{k+1} = 0$.

We now prove (1). Since $r_{k+1} = 0$, we have $r_{k-1} = r_kq_k$ and so $r_k \mid r_{k-1}$. Now, inductively assume $r_k \mid r_{i+1}$ and $r_k \mid r_{i+2}$. Since $r_i = r_{i+1}q_{i+2} + r_{i+2}$, we see $r_k \mid r_i$ as well. This proves that r_k divides all r_i, in particular it divides $r_{-1} = a$ and $r_0 = b$.

For (2), we prove by induction that there exist $s_i, t_i \in R$ with $as_i + bt_i = r_i$. For the base case of the induction, we have $a = r_{-1} \cdot 1 + r_0 \cdot 0$ and $b = r_{-1} \cdot 0 + r_0 \cdot 1$. We may therefore take $s_{-1} = 1$, $t_{-1} = 0$, $s_0 = 0$ and $t_0 = 1$. Now assume that there exists $s_{i-1}, t_{i-1}, s_i, t_i \in R$ with

$$as_{i-1} + bt_{i-1} = r_{i-1} \quad \text{and} \quad as_i + bt_i = r_i.$$

We will show the existence of $s_i, t_i \in R$ with $as_i + bt_i = r_i$. By definition, we have

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_iq_i \\ &= (as_{i-1} + bt_{i-1}) - (as_i + bt_i)q_i \\ &= a(s_{i-1} - q_is_i) + b(t_{i-1} - t_iq_i), \end{aligned}$$

so we may take $s_{i+1} = s_{i-1} - q_is_i$ and $t_{i+1} = t_{i-1} - t_iq_i$. We have therefore shown that every r_j is of the form $as_j + bt_j$ for some $s_j, t_j \in R$. In particular, the statement is true when $j = k$.

Now (3) follows from (2) since if $as + bt = r_k$, then any common divisor of a and b must also divide r_k. ■

1.8.13. Definition. Let $a, b \in R$ with R an integral domain. We say a and b are **relatively prime** if for every $e \in R$, $e \mid a$ and $e \mid b$ implies $e \in R^*$.

1.8.14. Example. When $R = \mathbb{Z}$, Definition 1.8.13 agrees with the usual notion of relative primality since $\mathbb{Z}^* = \{\pm 1\}$. In $\mathbb{Q}$, any two non-zero elements are relatively prime.

1.8.15. Corollary. *Let (R, f) be a Euclidean domain. Then $a, b \in R$ are relatively prime if and only if there exist $s, t \in R$ such that $as + bt = 1$.*

Proof. Suppose $as + bt = 1$. If $d \mid a$ and $d \mid b$, then $d \mid 1$ so $d \in R^*$. This shows a and b are relatively prime.

Conversely, applying Euclid's algorithm 1.8.12, we see there exist s, t, r_k in R with $as + bt = r_k$, $r_k \mid a$ and $r_k \mid b$. Since a and b are relatively prime, $r_k \in R^*$. Hence, $a(sr_k^{-1}) + b(tr_k^{-1}) = 1$. ■

We next show that every non-zero non-unit can be factored into a product of finitely many irreducibles. This gives an analogue of Theorem 1.3.3.

1.8.16. Proposition. *Let (R, f) be a Euclidean domain. Then every non-zero non-unit $a \in R$ is a product of finitely many irreducible elements.*

Proof. We do induction on $f(a)$. By Lemma 1.8.8 (1), $f(a) \geq f(1)$ for all $a \neq 0$. Let us begin with the base case of the induction, namely $f(a) = f(1)$. By Lemma 1.8.8 (3), we have $a \in R^*$ and so there is nothing to show.

Next, fix a number $n > 1$ and assume that the statement is true for all $b \in R$ with $1 \leq f(b) < n$. Then we will prove the statement for all a with $f(a) = n$. If a is irreducible then we are done. So, we may assume a is not irreducible, in which case, by definition, we have $a = bc$ with $b, c \notin R^*$. Then Lemma 1.8.8 (2) shows $f(b) < f(a)$ since $c \notin R^*$. Similarly, $f(c) < f(a)$. By our inductive hypothesis, we know both b and c are products of finitely many irreducible elements. Since $a = bc$, we can multiply these two factorizations together to obtain a as a product of finitely many irreducible elements. ■

We next prove an analogue of Corollary 1.6.2, which was the key input to showing the Fundamental Theorem of Arithmetic.

1.8.17. Proposition. *Let R be a Euclidean domain and suppose $p \in R$ is irreducible. If p divides the product $a_1 a_2 \dots a_k$, then there is an index j so that $p \mid a_j$.*

Proof. We proceed by induction on k. For $k = 1$, there is nothing to prove.

Now let $k = 2$. First suppose that p and a_1 are relatively prime. By Corollary 1.8.15, there exist $s, t \in R$ such that $1 = ps + a_1 t$. Therefore $a_2 = pa_2 s + a_1 a_2 t$. Since $p \mid a_1 a_2$, we get $p \mid a_2$. On the other hand, suppose p and a_1 are not relatively prime. Thus, there exists $d \notin R^*$ such that $d \mid p$ and $d \mid a_1$. By the definition of an irreducible element, we see $d = up$ where $u \in R^*$. Then $up = d \mid a_1$, so $p \mid a_1$. This completes the $k = 2$ case.

We now consider $k > 2$. We have $p \mid ba_k$, where $b = a_1 a_2 \dots a_{k-1}$. If $p \mid a_k$, we are done. Otherwise we may assume p does not divide a_k. Then by the $k = 2$ case, we see $p \mid a_1 a_2 \dots a_{k-1}$. By induction, there exists j such that $p \mid a_j$. ■

We now come to the main result of this section: in every Euclidean domain, we can uniquely factor elements as a product of irreducible elements.

1.8.18 Unique Factorization for Euclidean Domains. *Let (R, f) be a Euclidean domain. Then every non-zero non-unit $a \in R$ can be written as a product of finitely many irreducible elements. Moreover, if*

$$a = p_1 \dots p_r = q_1 \dots q_s$$

with all p_i, q_j irreducible, then $r = s$ and after reordering the q's, we have $q_i = u_i p_i$ for some $u_i \in R^*$.

Proof. By Proposition 1.8.16, we know that every non-zero non-unit a can be factored into a product of finitely many irreducible elements. To prove the unique factorization statement, we proceed by induction on $f(a)$. That is, we let $P(n)$ be the statement that the conclusion of the theorem is valid for every $a \in R$ with $f(a) = n$.

By Lemma 1.8.8 (1), we know $f(a) \geq f(1)$ for all non-zero a. Let us begin with the base case of the induction, namely $f(a) = f(1)$. By Lemma 1.8.8 (3), we have $a \in R^*$. Then if $p_1 \dots p_r = a$, we see $p_i \mid 1$, so $p_i \in R^*$ which contradicts the definition of an irreducible element. Therefore, a has no factorization into irreducible elements, and hence the statement $P(f(1))$ is vacuously true.

Next, assume that $f(a) = n > f(1)$ and $P(k)$ is true for $1 \leq k < n$. We will prove the statement for a. Assume that $a = p_1 \dots p_r = q_1 \dots q_s$ are two factorizations into irreducibles. Then

$$p_1 \mid a = p_1 \dots p_r = q_1 \dots q_s.$$

By Proposition 1.8.17, $p_1 \mid q_j$ for some j. After reordering the q's, we may suppose that $p_1 | q_1$. Since $p_1 \notin R^*$, using the definition of an irreducible element applied to q_1, we see $q_1 = u_1 p_1$ for some $u_1 \in R^*$. Therefore,

$$p_2 p_3 \dots p_r = \frac{a}{p_1} = q_2' q_3 \dots q_s,$$

where $q_2' = u_1 q_2$. Directly from the definition, we have that q_2' is also irreducible. Since $\frac{a}{p_1} \mid a$ and $p_1 \notin R^*$, we have from Lemma 1.8.8 (2) that $f(\frac{a}{p_1}) < f(a)$. By the induction hypothesis, we conclude that $r-1 = s-1$ (i.e. $r = s$) and after reordering the p_i, we have $q_2' = vp_2$ and $q_i = u_i p_i$ for some $v, u_i \in R^*$ for $3 \leq i \leq r$. Thus $q_2 = (u_1^{-1}v)p_2$; so we set $u_2 = u_1^{-1}v \in R^*$. This establishes $P(n)$. By induction, the proof is complete. ■

Exercises

1. Let $\mathbb{Q}[\sqrt{2}] = \{r + s\sqrt{2} : r, s \in \mathbb{Q}\}$. For $x = r + s\sqrt{2}$ in $\mathbb{Q}[\sqrt{2}]$, define the *norm* of x be $N(x) = r^2 - 2s^2 \in \mathbb{Q}$.
   (a) Show that $r + s\sqrt{2} = t + u\sqrt{2}$ for $r, s, t, u \in \mathbb{Q}$ implies $r = t$ and $s = u$.
   (b) Show that if $x, y \in \mathbb{Q}[\sqrt{2}]$ and $y \neq 0$, then $x/y \in \mathbb{Q}[\sqrt{2}]$.
   (c) Show that $N(x) = 0$ implies that $x = 0$ for x in $\mathbb{Q}[\sqrt{2}]$.
   (d) Show that $N(xy) = N(x)N(y)$ for all x, y in $\mathbb{Q}[\sqrt{2}]$.

2. (a) Show that $1 + \sqrt{2}$ and $17 + 12\sqrt{2}$ are units in $\mathbb{Z}[\sqrt{2}]$.
   (b) Prove that $x \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $N(x) = \pm 1$.
   HINT: $N(x)$ is an integer.
   (c) Prove that there are infinitely many units in $\mathbb{Z}[\sqrt{2}]$.
   HINT: find a way to make other units from $1 + \sqrt{2}$.

3. (a) Show that 2 and 7 are not irreducible in $\mathbb{Z}[\sqrt{2}]$.
   (b) Show that $x = 5 - 2\sqrt{2}$ is irreducible in $\mathbb{Z}[\sqrt{2}]$.
   HINT: compute $N(x)$.
   (c) Show that 3 is irreducible in $\mathbb{Z}[\sqrt{2}]$.
   HINT: What are the possible remainders after dividing a square by 8? Show that $N(x) = \pm 3$ is impossible.

4. Find a Euclidean function for $\mathbb{Z}[\sqrt{3}]$.
HINT: modify Example 1.8.11.

5. Let R be a ring. Suppose that $x \in R$ and there are elements $y_1, y_2 \in R$ such that $y_1 x = 1 = xy_2$. Prove that $y_1 = y_2$; and so x is a unit. In particular, if x is a unit, then it has a unique inverse.

6. Let f be a function on a ring R satisfying the division property of a Euclidean domain. Define $g(a) = \min\{f(ab) : b \neq 0\}$. Prove that g is a Euclidean function for R.

7. (a) Prove that $(\mathbb{Q}, f)$ is a Euclidean domain, where $f(0) = 0$ and $f(a) = 1$ for $0 \neq a \in \mathbb{Q}$.
   (b) More generally, let F be a commutative ring such that $F^* = F \setminus \{0\}$; such a ring F is called a *field*. Set $f(0) = 0$ and $f(a) = 1$ for all $a \neq 0$. Prove that f is a Euclidean function for F.

8. Let (R, f) be a Euclidean domain. Let $g : \operatorname{Ran} f \to \mathbb{N}_0$ be any strictly increasing function. Prove that $g \circ f$ is also a Euclidean function for R.

9. (a) Show that $\mathbb{Z}[\sqrt{2}]$ is '*dense*' in $\mathbb{R}$, meaning that if $x < y$ in $\mathbb{R}$, then there are integers a, b so that $x < a + b\sqrt{2} < y$.
HINT: for each $n \in \mathbb{N}$, there is some $a_n \in \mathbb{Z}$ so that $a_n + n\sqrt{2} \in (0, 1)$. Choose k so that $\frac{1}{k} < y - x$. Use the pigeonhole principle to find two numbers $m < n$ so that $0 < |(a_n + n\sqrt{2}) - (a_m + m\sqrt{2})| < \frac{1}{k}$.
(b) Explain why the order on $\mathbb{Z}[\sqrt{2}]$ induced from $\mathbb{R}$ cannot be used to define a Euclidean function.

Notes on Chapter 1

Presumably numbers arose from counting. Once civilizations developed some mode of writing, they also developed ways to record numbers. The ancient Egyptians had a system for writing numbers up to a million. The ancient Chinese had a base 10 system of numbers. Babylonians developed a system base 60.

The notion of zero came later, first as a placeholder for writing numbers in base 10. For example, the Chinese just left a blank space for a zero in a base 10 number. The Babylonians first left it to context, but eventually adopted a symbol to indicate a blank space around 400 BCE. The Greeks however did not adopt the concept. The symbol zero apparently comes from India, possibly as early as 200 CE. It was brought back to Europe by the Arabs, who adopted it. Around 700 CE, Brahmagupta gave arithmetic rules for working with 0 as a number in its own right. This spread to China, with records from 1247 CE. Around this time, Fibonacci was proposing the use of 0. It wasn't until the 1600s that 0 came into more common usage in Europe.

Negative numbers were not generally accepted in ancient times. There is a record of the use of negative numbers for solving equations in China around 100 BCE–50 CE. In Greece, in the third century, Diophantus made use of negative numbers as 'a number to be subtracted' for use in solving equations. However he apparently did not accept them as numbers on their own. In the 7th century, Brahmagupta used negative numbers to reduce the solution of a quadratic equation to a single case. (Diophantus had three cases.) Records from China show negative numbers in use by the 13th century. In 1545, Cardano used negative numbers in his formulae for roots of cubics and quartics. In the 17th century, Descartes partially accepted negative numbers, although he considered them as false solutions to equations. In the 18th century, Euler discussed operations with positive and negative numbers. Yet still in the 19th century, Hamilton attempted 'to put negative numbers on a firm theoretical footing'. By this time, it was becoming more accepted—a surprisingly long time!

Euclid wrote a 13 volume treatise on mathematics in 300 BCE. It contains the Euclidean algorithm and the proof of an infinitude of primes. It

also contains Lemma 1.6.1 and Corollary 1.6.2. As we saw, it is a small step from these results to the Fundamental theorem of arithmetic—but it does not appear in Euclid. The first precise statement of the FTA is by Gauss in 1801.

The Euclidean algorithm for the Gaussian integers was known to Gauss (see Section 3.5). Generally people only considered Euclidean algorithms for the norm function until 1950. The abstract notion of a Euclidean domain was implicit in work by Hasse in 1928.

Hardy and Wright [**15**] is a classic book on number theory that is still relevant today. It differs from many number theory books in that it often discusses different proofs, and it contains many historical notes. The 6th edition has updated notes that reference many more recent results. Ribenboim's *The little book of bigger primes* [**31**] is, as the title suggests, all about primes. There are many proofs of the infinitude of primes in Chapter 1. Stark [**37**] is a more modern number theory book whose introduction, in particular, is well worth reading by readers of our book. Silverman [**34**] is another nice introduction to number theory.

Alaca and Williams [**2**] is an algebraic number theory book which treats Euclidean domains in general. In particular, they give many results about the quadratic number domains $\mathbb{Z}[\sqrt{d}]$ for $d \equiv 2, 3 \pmod 4$ and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ when $d \equiv 1 \pmod 4$. We explain at the end of Section 3.3 why we use $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ rather than $\mathbb{Z}[\sqrt{d}]$ when $d \equiv 1 \pmod 4$. Stark [**37**, Section 8.4] also has interesting material about when quadratic number domains are Euclidean or UFD (unique factorization domains), which is a strictly larger class. Stark himself made important contributions to this problem.

Chapter 2

Modular Arithmetic

In this chapter, we discuss computations '*modulo* n', meaning that we only keep track of the remainder on division by n. We discuss solving systems of equations in several interesting contexts.

2.1. Linear Equations

In this section, we look for integer solutions of the simplest type of equations. An equation in which one searches for integer solutions is called a Diophantine equation, after the Greek mathematician Diophantus. Consider the equation

$$ax + by = c$$

where a, b and c are given integers. For example, $5x+7y = 1$ has the solution $x = 3$ and $y = -2$. But $6x + 10y = 15$ has no solutions because the left side is even, and 15 is odd. In general, $ax+by$ is always divisible by $d = \gcd(a, b)$. Thus a *necessary condition* for a solution is

$$\gcd(a, b)|c.$$

This is also *sufficient*. It follows from the Euclidean algorithm that there are integers s and t so that $as + bt = d$. So if $c = dz$, a solution of our equation is given by $x = sz$ and $y = tz$. Therefore we have proved most of the following theorem.

2.1.1. Theorem. *The Diophantine equation $ax + by = c$ has a solution if and only if $d = \gcd(a, b)$ divides c. Moreover, if $\{x_0, y_0\}$ is one solution, then all solutions are given by*

$$x = x_0 + k\frac{b}{d} \qquad y = y_0 - k\frac{a}{d} \qquad \text{for} \quad k \in \mathbb{Z}.$$

Proof. The first part has been done. So suppose that $\{x_0, y_0\}$ and $\{x, y\}$ are solutions of $ax + by = c$. Then $X = x - x_0$ and $Y = y - y_0$ satisfy

$$aX + bY = (ax + by) - (ax_0 + by_0) = 0.$$

Hence $aX = -bY$. Dividing by $d = \gcd(a, b)$ yields $\frac{a}{d}X = -\frac{b}{d}Y$. But, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Thus by Lemma 1.6.1, $\frac{a}{d}|Y$ and $\frac{b}{d}|X$. Set $k = \dfrac{Xd}{b}$. So

$$x = x_0 + X = x_0 + k\frac{b}{d}.$$

It follows that $Y = -\frac{a}{b}X = -k\frac{a}{d}$, and thus

$$y = y_0 + Y = y_0 - k\frac{a}{d}.$$

Conversely, it is clear that every pair $\{x, y\}$ of this form is a solution. ■

Now we can handle more variables with a simple induction argument. If $a_1, \ldots, a_n$ are integers which are not all 0, then we denote the greatest common divisor of a set $\{a_1, \ldots, a_n\}$ by $\gcd(a_1, \ldots, a_n)$. We define $\gcd(0, \ldots, 0) = 0$. Like the Euclidean algorithm (1.5.4), Corollary 2.1.2 gives a *constructive* method for finding solutions to the Diophantine equation $\sum_{i=1}^{n} a_i x_i = c$.

2.1.2. Corollary. *Let $a_1, \ldots, a_n \in \mathbb{Z}$. The Diophantine equation*

$$\sum_{i=1}^{n} a_i x_i = c$$

has a solution if and only if $\gcd(a_1, \ldots, a_n)|c$.

Proof. If $a_1 = \ldots = a_n = 0$, then there is a solution to $\sum_{i=1}^{n} a_i x_i = c$ if and only if $c = 0$. We see $c = 0$ if and only if $0 \mid c$, and since $\gcd(0, \ldots, 0) = 0$, the corollary holds in this case.

Hence for the remainder of the proof, we may assume some $a_i \neq 0$, in which case $d = \gcd(a_1, \ldots, a_n)$ is the greatest common divisor of the set $\{a_1, \ldots, a_n\}$.

The case $n = 1$ is trivial, and the $n = 2$ case is a consequence of Theorem 2.1.1. Proceeding by induction, we suppose that the result holds for $n = k-1$ (and $n = 2$). Consider the equation

$$\sum_{i=1}^{n} a_i x_i = c.$$

Since d divides the left-hand side of this equation, the condition $d|c$ is necessary.

Suppose that $d|c$. Let $b = \gcd(a_1, \ldots, a_{n-1})$, and note that $\gcd(b, a_n) = d$. By the $n = 2$ case, the equation $by + a_n x_n = c$ has a solution, say $y = Y$ and $x_n = X_n$. Now using the $n = k - 1$ case, since $b|bY$, solve the equation

$$\sum_{i=1}^{n-1} a_i x_i = bY.$$

Call this solution $x_i = X_i$ for $i = 1, \ldots, n-1$. It is clear that $X_1, \ldots, X_n$ is a solution to our original equation. ■

2.1.3. Example. Consider the problem of measuring exactly 3 cups of water using two containers, one which holds 12 cups and one which holds 17 cups, but neither has any markings for smaller units. This is really a matter of solving the equation $12x + 17y = 3$. From the Euclidean algorithm, we get $5(17) - 7(12) = 1$. (See the table.)

n	q	s	t
17		1	0
12		0	1
5	1	1	-1
2	2	-2	3
1	2	5	-7

Hence, $3 = 15(17) - 21(12) = 3(17) - 4(12)$. To implement this solution, fill the 17 cup container. Fill the 12 cup container from the 17 cupper. Dump out the 12 cup container and add the remaining 5 cups. Refill the 17 cup container, and continue filling and emptying the 12 cup container. It takes another 7 cups to fill it. Empty the 12 cup container again, and add the remaining 10 cups. Fill the 17 cupper a third time. Two more cups fills the 12 cupper, leaving 15 cups in the 17 cup container. Pour out another 12 cups, leaving the 17 cup container holding exactly 3 cups. In other words, we have filled the 17 cup container 3 times, and emptied out 4 lots of 12 cups using the 12 cup container. This leaves $3(17) - 4(12) = 3$ cups.

Exercises

1. Solve $615x + 243y = 21$.

2. Solve $2491x + 1113y = 212$.

3. Using a 16 cL measure and a 27 cL measure and (approximately) half a litre of milk in a jug, how can you measure out exactly 30 cL? What is the most efficient way?

4. Find a solution of $30w + 42x + 70y + 105z = 1$.

5. An experimental robot may move forward in small steps of 27cm and in large steps of 75cm. It cannot turn or move backwards. It is at the beginning of a track of length exactly 10m. How does the robot get as close as possible to the other end of the track?

6. A revised version of the robot above is able to move backwards as well as forwards the same distances. How much better can it do on a short track of length 1m than the earlier model robot?

2.2. Congruences

A rather useful notion in number theory is that of **modular arithmetic**, which means, working only with the remainders after division by some fixed integer. For example, working *modulo 2*, a number is either even or odd. To determine the parity of the sum of two numbers, one need only know the parity of the the two numbers, not their actual values. Similarly, their product will be even if either number is even, and odd only if both are odd. Assign the number 0 to all even numbers (as this is the remainder after dividing by 2), and assign the number 1 to all odd numbers. The 'addition' and 'multiplication' tables for these remainders is the one given in section 1.1 for the ring $\mathbb{Z}_2$.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Another familiar situation is clock arithmetic. If the time now is 7 o'clock, then in 19 hours it will be 2 o'clock. This calculation amounts to adding 19 to 7, and then throwing away all multiples of 12 until the result lies in the range of 1 to 12.

We will see that a similar situation holds for every positive integer n. We say that a is **congruent** to b **modulo** n provided that n divides $a - b$, and write

$$a \equiv b \pmod{n}.$$

For example,

$$\begin{aligned} 752 &\equiv 968352 \pmod{100} \\ \text{-}98743 &\equiv 57 \pmod{16} \end{aligned}$$

but

$$99998 \not\equiv 22 \pmod{3}$$

For every integer a, the Division algorithm shows that there is exactly one number b in $\{0, 1, \ldots, n-1\}$ so that $a \equiv b \pmod{n}$. For each remainder $\mathbf{a}$, an integer a can be chosen so that $a \equiv \mathbf{a} \pmod{n}$ called a **representative** of $\mathbf{a}$. The important property to recognize is that addition and multiplication of remainders does not depend on which representative is used. More precisely:

2.2.1. Proposition. *Let n be a positive integer. Suppose that $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then,*

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n},$$

and

$$a_1 b_1 \equiv a_2 b_2 \pmod{n}.$$

Proof. The hypotheses say that n divides both $a_1 - a_2$ and $b_1 - b_2$. Adding shows that n divides

$$(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2),$$

which is to say, $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$.

For multiplication, consider the calculation

$$a_1 b_1 - a_2 b_2 = (a_1 - a_2)b_1 + a_2(b_1 - b_2).$$

Since $a_1 - a_2$ and $b_1 - b_2$ are multiples of n, this shows that $a_1 b_1 - a_2 b_2$ is a multiple of n. In other words, $a_1 b_1 \equiv a_2 b_2 \pmod{n}$. ■

For example, consider the problem of determining the last 2 digits of 311^{1243}. Since $311 \equiv 11 \pmod{100}$, it suffices to consider powers of 11. These powers are computed modulo 100 as 11,21,31,41,.... It is not necessary to compute 11^3, for example, because

$$11^3 \equiv 21 \cdot 11 = 231 \equiv 31 \pmod{100}.$$

In particular, $11^{10} \equiv 1 \pmod{100}$. Thus,

$$311^{1243} \equiv (11^{10})^{124}(11^3) \equiv 31 \pmod{100}.$$

Later on, we will derive computational tools that will make this exercise even easier.

Exercises

1. Compute the remainder modulo 7 of 2222^{5555}.

2. What are the possible squares modulo 4? Hence show that 1234567 is not the sum of two squares.

3. Suppose that $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Show that

$$a_1 - b_1 \equiv a_2 - b_2 \pmod{n}.$$

4. Suppose that $a \equiv b \pmod{n}$. If $p(x)$ is a polynomial with integer coefficients, show that

$$p(a) \equiv p(b) \pmod{n}.$$

HINT: First prove this for the monomials x^n.

5. Let $n = \sum_{i=0}^{\ell} a_i 10^i$ where the a_i are positive integers in $\{0, 1, \ldots, 9\}$, i.e., when written in base-10 expansion, n has digits $a_\ell, \ldots, a_0$.

(a) Prove that $3 \mid n$ if and only if $3 \mid \sum_{i=0}^{\ell} a_i$.

(b) Prove that $9 \mid n$ if and only if $9 \mid \sum_{i=0}^{\ell} a_i$.

(c) Prove that $11 \mid n$ if and only if $11 \mid \sum_{i=0}^{\ell} (-1)^i a_i$.

(d) Give a criterion in terms of the digits a_i for when 7 divides n.
HINT: $7 \mid 1001$.

6. (Josephus Problem) Let n be a positive integer and write the numbers from 1 through n in a circle. Starting at 1, continue going around the circle removing every other number until only one number remains. Determine the values of n for which 1 is the last remaining number. For example, if $n = 7$, we start by crossing off 2, then 4, then 6, then 1, then 5, then 3, so the last remaining number is 7.

2.3. The Ring $\mathbb{Z}_n$

Proposition 2.2.1 allows us to define a ring called $\mathbb{Z}_n$. The elements of the ring are $[0], [1], \ldots, [n-1]$ corresponding to the remainders $\{0, \ldots, n-1\}$. Addition is defined by setting $[a] + [b]$ to be the remainder $[c]$ such that $a + b \equiv c \pmod{n}$. Similarly, multiplication is defined by setting $[ab]$ to be the remainder $[c]$ such that $ab \equiv c \pmod{n}$.

2.3.1. Example. Here are addition and multiplication tables for $\mathbb{Z}_4$ and $\mathbb{Z}_5$:

$\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5$:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Alternatively, we can use all the integers to represent elements $[k]$ of $\mathbb{Z}_n$ with the rule that $[j] = [k]$ if and only if $j - k \equiv 0 \pmod{n}$. Then the rules for addition and multiplication become

$$[j] + [k] = [j + k] \qquad [j][k] = [jk].$$

This appears easier, but it raises a new difficulty. Before, there was only one definition of addition and multiplication for each pair $\{[a], [b]\}$. Now there are many such definitions, one for each pair of integers which represent the same two elements. It is important that all these definitions agree. For example, consider $[2] + [3] = [5]$ in $\mathbb{Z}_7$. Instead, one might have chosen representatives $[16]$ instead of $[2]$ and $[-18]$ instead of $[3]$. For their sum, we get $[16] + [-18] = [-2]$. Since $[-2] = [5]$ in $\mathbb{Z}_7$, these two definitions are the same. Proposition 2.2.1 shows that we get the same result regardless of which representative is chosen.

Using these tables, we can painstakingly verify all the laws of a commutative ring. However, a bit of thought shows that $\mathbb{Z}_5$ *inherits* all these properties from the integers. For example, consider the associative law for addition. For any elements $[a], [b], [c]$ in $\mathbb{Z}_5$,

$$\begin{aligned}[a] + ([b] + [c]) &= [a] + [b + c] = [a + (b + c)] \\ &= [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c].\end{aligned}$$

Proposition 2.2.1 shows that it did not matter which choice of representatives was made. So the formula is verified. Similarly, all the properties of a commutative ring can be verified. So we obtain:

2.3.2. Proposition. *$\mathbb{Z}_n$ is a commutative ring.*

If you study the multiplication table for $\mathbb{Z}_5$ above, you will see that every non-zero element has an **inverse**; for example, $[2] \cdot [3] = [1]$. (That is, $2(3) = 6 \equiv 1 \pmod 5$.) This is a property which $\mathbb{Z}_5$ has but the integers do not. A commutative ring in which every non-zero element has an inverse is called a **field**. These fields will play a very important role in algebra. Two well known fields are the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$.

In Definition 1.8.1, we defined integral domains and zero divisors. Fields are examples of integral domains, but $\mathbb{Z}$ is an example of an integral domain which is not a field. The ring $\mathbb{Z}_6$ provides an example of a ring which is not an integral domain since [2] and [3] are zero divisors; this is because $[2] \cdot [3] = [6] = [0]$ but $[2] \neq [0] \neq [3]$.

In order to determine when $\mathbb{Z}_n$ is a field, we need the following simple consequence of the Euclidean algorithm.

2.3.3. Lemma. *Suppose that a, b and n are integers with $\gcd(a, n) = 1$. Then the equation*

$$ax \equiv b \pmod n$$

has exactly one integer solution modulo n. In other words, $[a][x] = [b]$ has exactly one solution in $\mathbb{Z}_n$.

Proof. Define a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f([x]) = [ax]$ for all $[x]$ in $\mathbb{Z}_n$. First, let us verify that f is one-to-one. Suppose that $[x]$ and $[y]$ are elements of $\mathbb{Z}_n$. Pick representatives x and y in $\mathbb{Z}$ for $[x]$ and $[y]$. If $f([x]) = f([y])$, we can interpret this as saying $ax \equiv ay \pmod n$. This is equivalent to saying that n divides $a(x - y)$. By Lemma 1.6.1, n divides $x - y$. This of course means that $x \equiv y \pmod n$. So, $[x] = [y]$.

The set $\mathbb{Z}_n$ has exactly n elements. The function f is one-to-one, and so takes each of these n elements to n distinct elements of $\mathbb{Z}_n$. It follows that f is onto. Thus there is exactly one element $[x_0]$ such that $[b] = f([x_0]) = [ax_0]$. In other words, x_0 is the unique solution mod n of the congruence equation $ax \equiv b \pmod n$. ■

2.3.4. Corollary. *For integers a and n, there is an integer b so that $ab \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$.*

Proof. The 'if' direction is immediate from the lemma. On the other hand, if $\gcd(a, n) = d > 1$, then $ab + kn$ is a multiple of d for every choice of b and k; and so can never equal 1. ■

The invertible elements of a ring are called **units**. The set $\mathbb{Z}_n^*$ of all units of $\mathbb{Z}_n$ is called the **group of units** of $\mathbb{Z}_n$. $\mathbb{Z}_n^*$ is closed under multiplication (i.e. if $[a]$ and $[b]$ are units, then $[ab]$ is a unit). It has an identity $[1]$, every element has an inverse, and multiplication is commutative and associative. An algebraic object with these properties is called an **abelian group**. (The word abelian is derived from the name **Abel**, who was an eminent algebraist. It means commutative.)

This corollary shows that $[a]$ is an invertible element, or unit of $\mathbb{Z}_n$ exactly when $\gcd(a, n) = 1$. We record this as a separate result.

2.3.5. Corollary. *The units of $\mathbb{Z}_n$ are $\mathbb{Z}_n^* = \big\{[a] : \gcd(a, n) = 1\big\}$.*

Now we can show that $\mathbb{Z}_n$ is a field if and only if n is a prime.

2.3.6. Theorem. *If p is a prime, then $\mathbb{Z}_p$ is a field. On the other hand, if n is composite, $\mathbb{Z}_n$ has zero divisors and hence is not an integral domain.*

Proof. Suppose p is prime. Then every non-zero element of $\mathbb{Z}_p$ has an inverse by Corollary 2.3.5. Hence $\mathbb{Z}_p$ is a field.

Conversely, if n is composite, factor $n = ab$ so that neither a nor b is $\pm n$. Then n does not divide either a or b. So they represent non-zero elements $[a]$ and $[b]$ in $\mathbb{Z}_n$ satisfying $[a][b] = [0]$. Therefore $\mathbb{Z}_n$ has zero divisors. ■

The final result of this section gives a bound on the number of roots of a polynomial in $\mathbb{Z}_p$. We prove this after a preliminary lemma.

2.3.7. Lemma. *Let $a \in \mathbb{Z}$ and*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_0, \ldots, a_n \in \mathbb{Z}$. Then there is a polynomial $q(x)$ and $r \in \mathbb{Z}$ so that $p(x) = (x - a)q(x) + r$. Moreover, $r = p(a)$.

Proof. We prove the existence of $q(x)$ and r by induction on n. If $n = 0$, we may take $q = 0$ and $r = a_0$. For $n > 0$, we achieve the result by "long division". We have $(x - a)a_n x^{n-1} = a_n x^n - a a_n x^{n-1}$ is a multiple of $x - a$. Subtracting this from $p(x)$ leaves

$$p_1(x) = (a_{n-1} + a a_n) x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0.$$

By our inductive hypothesis, we have a polynomial $q_1(x)$ in $\mathbb{Z}[x]$ and $r \in \mathbb{Z}$ such that $p_1(x) = (x-a)q_1(x) + r$. Then

$$p(x) = p_1(x) + (x-a)a_n x^{n-1} = (x-a)(q_1(x) + a_n x^{n-1}) + r,$$

so we may take $q(x) = q_1(x) + a_n x^{n-1}$. Since $p(x) = (x-a)q(x) + r$, substituting $x = a$ yields $r = p(a)$. ■

A polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is **monic** if $a_n = 1$.

2.3.8. Corollary. *If $q(x)$ is a monic polynomial of degree d with integer coefficients, and p is a prime, then the congruence equation*

$$q(x) \equiv 0 \pmod{p}$$

has at most d solutions modulo p.

Proof. This will follow by induction on the degree d. For $d = 1$, this follows from Lemma 2.3.3. Assume that the result holds for all polynomials of degree less than d. If $q(x) \equiv 0 \pmod{p}$ has no solutions, the theorem holds trivially. So assume that a is a solution, By Lemma 2.3.7, we have

$$q(x) = (x-a)q_1(x) + q(a) \equiv (x-a)q_1(x) \pmod{p}.$$

If $b \not\equiv a \pmod{p}$ is any other solution, then

$$0 \equiv q(b) \equiv (b-a)q_1(b) \pmod{p}.$$

Since $b - a \not\equiv 0 \pmod{p}$ and $\mathbb{Z}_p$ has no zero divisors, it follows that $q_1(b) \equiv 0 \pmod{p}$. In other words, all roots of q other than a are roots of q_1. By the induction hypothesis, $q_1(x) \equiv 0 \pmod{p}$ has at most $d-1$ solutions. Therefore $q(x) \equiv 0 \pmod{p}$ has at most d solutions. ■

Exercises

1. Write down the addition and multiplication tables for $\mathbb{Z}_6$.

2. Solve the equation $x^2 + 4x + 2 \equiv 0 \pmod{7}$ by completing the square.

3. Solve the equation $x^2 + x + 7 \equiv 0 \pmod{13}$ by completing the square. In this case, it helps to add a linear polynomial which is congruent to 0 modulo 13.

4. Show by example that Corollary 2.3.8 is false if p is not prime.

5. Show by example that Corollary 2.3.8 is false if q is not monic.[1]

6.★ Show that every finite integral domain is a field.
HINT: modify the proof of Lemma 2.3.3.

[1] We thank Anton Mosunov for suggesting this exercise.

2.4. Equivalence Relations

In this section, we will discuss an important mathematical notion which was used implicitly in the last two sections. This topic could be skipped by those keen to get on with the number theory. However, it is a notion that will recur frequently in your mathematical studies.

2.4.1. Definition. An **equivalence relation** on a set S is a relation $\approx$ satisfying the three properties:

(1) **reflexivity:** $a \approx a$ for all $a \in S$.
(2) **symmetry:** $a \approx b$ implies $b \approx a$ for all $a, b \in S$.
(3) **transitivity:** $a \approx b$ and $b \approx c$ imply $a \approx c$ for all $a, b, c \in S$.

2.4.2. Example. Let S be any set, and consider the equality relation. That is, a is related to b if and only if $a = b$. This is easily seen to be an equivalence relation.

2.4.3. Example. Consider the relation on $\mathbb{Z}$ given by congruence modulo n. It is clear that the reflexivity property $a \equiv a \pmod{n}$ holds since $n|0$. Also, if $a \equiv b \pmod{n}$, then $n|b-a$. Thus, $n|a-b$ and so $b \equiv a \pmod{n}$. This verifies symmetry. Finally, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $n|b-a$ and $n|c-b$, so $n|(c-b)+(b-a) = c-a$. Thus, $a \equiv c \pmod{n}$. So the relation is also transitive. This is an equivalence relation.

2.4.4. Example. Consider the relation $\leq$ on $\mathbb{R}$. Since $a \leq a$, we see $\leq$ is reflexive. If $a \leq b$ and $a \neq b$, then $b \not\leq a$. So $\leq$ is not symmetric. It is transitive, since $a \leq b$ and $b \leq c$ implies $a \leq c$. This is not an equivalence relation.

2.4.5. Example. Consider a relation on $\mathbb{Z}$ given by $n \approx m$ if n and m have the same sign, meaning $+$,$-$, or 0. Now, n has the same sign as itself. If n and m have the same sign, then m and n have the same sign. Finally, if n and m have the same sign, and m and k have the same sign, then n and k have the same sign. So, this is an equivalence relation.

If $\approx$ is an equivalence relation on a set S, then each element a of S belongs to the **equivalence class** $[a] = \{b \in S \mid b \approx a\}$. Every element of S belongs to exactly one equivalence class. So S is partitioned into a disjoint union of these equivalence classes. Conversely, if S is partitioned into a disjoint union of sets E_α for $\alpha \in A$, then define a relation $a \approx b$ if and only if a and b belong to the same set E_α. One can check that this is an equivalence relation. In fact, this is essentially what occurs in example

2.4.5 above. One denotes the set of equivalence classes by

$$\{[a] : a \in S\} = S/\approx$$

Equivalence relations arise naturally in many mathematical situations. Often, as is the case for modular arithmetic, one wants to define some algebraic operation on the equivalence classes which is compatible with the corresponding operation on the original set. Consider congruence modulo n again. The equivalence class for an integer a is $[a] = \{a + kn \,|\, k \in \mathbb{Z}\}$. When addition is defined on these equivalence classes by

$$[a] + [b] = [a + b],$$

it is important that we can choose *any* representative from each class and add them in order to determine the class of the sum. This is known as showing that the definition of addition is **well defined**. This is the content of Proposition 2.2.1. In other words,

$$\{a + jn \,|\, j \in \mathbb{Z}\} + \{b + kn \,|\, k \in \mathbb{Z}\} = \{a + b + tn \,|\, t \in \mathbb{Z}\}.$$

This same proposition shows that multiplication is well defined. In set terms,

$$\{a + jn \,|\, j \in \mathbb{Z}\} \cdot \{b + kn \,|\, k \in \mathbb{Z}\} \subset \{ab + tn \,|\, t \in \mathbb{Z}\}.$$

For contrast, consider defining addition in example 2.4.5. Let us call the three equivalence classes $[+]$, $[-]$ and $[0]$. When we try to define $[a] + [b] = [a + b]$, the sign of $a + b$ is ambiguous. For if $a = 1$ and $b = -2$, the sum is negative which suggests that $[+] + [-] = [-]$. But $a = 2$ and $b = -1$, then $a + b > 0$ which suggests $[+] + [-] = [+]$. Likewise, if $a = 3$ and $b = -3$, then $a + b = 0$ which suggests that $[+] + [-]$ should be $[0]$. So it is not possible to define an addition on these equivalence classes which is compatible with addition on the integers. Such a definition only works for certain equivalence relations. For this reason, when one defines an operation on equivalence classes, it is very important to check that the definition is well defined.

Exercises

1. Which of the following relations are equivalence relations? If not, determine which of the three properties do hold.

(a) For all $x, y \in \mathbb{R}$, say $x \approx y$ if $x - y$ is rational.

(b) For all $a, b \in \mathbb{Z}$, say $a \approx b$ if gcd $(a, b) = 1$.

(c) For all continuous, positive functions f, g on $\mathbb{R}$, say $f \approx g$ if

$$\lim_{x \to \infty} f(x)/g(x) = 1.$$

(d) For all $a, b \in \mathbb{Z}$, say $a \approx b$ if $3|(a + b)$.

(e) For all $a, b \in \mathbb{N}$, say $a \approx b$ if $a|b$.

2. Say that two continuous functions on $[0,1]$ are equivalent ($f \approx g$) provided that $f(0) = g(0)$ and $f(1) = g(1)$. Show that addition is well defined on the equivalence classes.

3. Put a relation on $\mathbb{N}$ by setting $n \approx m$ if $n/\gcd(n,m)$ and $m/\gcd(n,m)$ are both odd.
(a) Show that this is an equivalence relation, and describe the equivalence classes.
(b) Show that the multiplication $[n][m] = [nm]$ is well defined.
(c) Show that the addition $[n] + [m] = [n+m]$ is not well defined.

4. (Construction of the rational numbers) Put a relation on $S = \mathbb{Z} \times (\mathbb{Z} \smallsetminus 0)$ given by $(a,b) \approx (c,d)$ if $ad = bc$.
(a) Show that $\approx$ is an equivalence relation and let $Q = S/\approx$.
(b) Show that multiplication $[(a,b)][(c,d)] = [(ac,bd)]$ is well defined.
(c) Show that addition $[(a,b)] + [(c,d)] = [(ad+bc,bd)]$ is well defined.
(d) Prove that Q is a field with the above addition and multiplication operations.
(e) Prove that map

$$\varphi\colon Q \to \mathbb{Q}, \qquad \varphi([a,b]) = \frac{a}{b}$$

is an isomorphism.

5. (Construction of fraction fields) Let R be any integral domain and put a relation on $S = R \times (R \smallsetminus 0)$ given by $(a,b) \approx (c,d)$ if $ad = bc$.
(a) Show that $\approx$ is an equivalence relation and let $\mathrm{Frac}(R) = S/\approx$.
(b) Show that multiplication $[(a,b)][(c,d)] = [(ac,bd)]$ is well defined.
(c) Show that addition $[(a,b)] + [(c,d)] = [(ad+bc,bd)]$ is well defined.
(d) Prove that $\mathrm{Frac}(R)$ is a field with the above addition and multiplication operations. This is referred to as the *fraction field* (or *quotient field*) of R.

2.5. Chinese Remainder Theorem

In this section, we will study systems of linear congruences of a very special form. Problems of this type were studied in many ancient civilizations. A full solution was obtained first in China by Yih-hing in 717. It is thought to have been used as a method of representing numbers, and doing large computations.

To illustrate the method, consider the following example.

2.5.1. Example. Consider the system

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 12 \pmod{25} \\ x &\equiv 1 \pmod 3 \end{aligned}$$

First, let us solve the first pair of equations. This requires integers x, y and z such that

$$x = 3 + 4y = 12 + 25z.$$

Hence, $4y - 25z = 9$. By inspection, $y = -4$ and $z = -1$ is a solution. Since $\gcd(4, 25) = 1$, the most general solution is

$$y = -4 + 25m \qquad z = -1 + 4m.$$

Hence $x = 3 + 4(-4 + 25m) = -13 + 100m$. Now combine this with the third equation $x = 1 + 3n$. This yields

$$100m - 3n = 14.$$

Since $100(1) - 3(33) = 1$, there is a solution $m = 14$ and $n = 14(33) = 462$; hence, $m = 14 - 4(3) = 2$ and $n = 462 - 4(100) = 62$ is a solution. The most general solution is given by

$$m = 2 + 3k \qquad n = 62 + 100k,$$

which gives $x = 3(62 + 100k) + 1 = 187 + 300k$. In other words, $x \equiv 187 \pmod{300}$. Notice that $300 = (4)(25)(3)$.

Now we consider the problem in general.

2.5.2. Lemma. *Suppose that m and n are relatively prime positive integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a unique solution $\pmod{mn}$.

Proof. An integer x is a solution if and only if there are integers y and z satisfying

$$x = a + my = b + nz.$$

Therefore, y and z form a solution of

$$my - nz = b - a.$$

By Theorem 2.1.1, this has a solution y_0, z_0, and the most general solution is

$$y = y_0 + nk \qquad z = z_0 + mk.$$

Substituting back in yields

$$x = a + my_0 + mnk = b + nz_0 + mnk.$$

It is readily apparent that such an x solves our system of equations, so we have found a complete solution. From the form of this solution, x is unique modulo mn. ■

Now we can prove the Chinese Remainder Theorem.

2.5.3 Chinese Remainder Theorem. *Suppose that $m_1, \ldots, m_n$ are pairwise relatively prime positive integers (i.e. $\gcd(m_i, m_j) = 1$ for $i \neq j$). Then the system of congruence equations*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m_1 m_2 \ldots m_n$.

Proof. The proof is an induction argument. The lemma did the $n = 2$ case. Suppose that the result holds for all $k < n$, where $n \geq 3$. Consider the first $n-1$ equations. By the induction hypothesis, this system has a unique solution b modulo $m_1 \ldots m_{n-1}$. In other words, the solution of this system is the same as the solution of the equation

$$x \equiv b \pmod{m_1 \ldots m_{n-1}}.$$

So our original system has the same solutions as the system

$$\begin{aligned} x &\equiv b \pmod{m_1 \ldots m_{n-1}} \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

By the lemma, this has a unique solution $\pmod{m_1 \ldots m_n}$. ■

Exercises

1. Show that if $m_1, \ldots, m_n$ are not relatively prime, then the conclusion of the Chinese Remainder Theorem *never* holds.

2. Solve the system of equations

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 5 \pmod{11} \\ x &\equiv 9 \pmod{13}. \end{aligned}$$

3. Solve the system of equations

$$\begin{aligned} x &\equiv 9 \pmod{27} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 7 \pmod{16}. \end{aligned}$$

4. Solve the equation $x^3 - x - 1 \equiv 0 \pmod{385}$.

5. For every positive integer n, find n consecutive integers none of which are square-free.[2]

[2]This exercise was given on the 1955 Putnam competition.

2.6. Congruence Equations

Solving equations with congruences often yields useful information about the solution in the integers. It is also of independent interest to solve equations in $\mathbb{Z}_n$. Lemma 2.3.3 is an example of this kind of result. We will start by giving a more general form of it.

2.6.1. Theorem. *The congruence equation*

$$ax \equiv b \pmod{n}$$

has a solution if and only if $d = \gcd(a, n)$ *divides* b. *The solution is unique* $\pmod{n/d}$.

Proof. Notice that $ax \equiv b \pmod{n}$ if and only if there is an integer y such that $ax + ny = b$. By Theorem 2.1.1, this has a solution if and only if $\gcd(a, n)|b$. In this case, let $A = a/d$, $B = b/d$ and $N = n/d$. Dividing the Diophantine equation by d reduces the problem to solving $Ax + Ny = B$. This is equivalent to solving $Ax \equiv B \pmod{N}$. Since $\gcd(A, N) = 1$, Lemma 2.3.3 shows that the solution is unique $\pmod{N}$. ■

2.6.2. Example. Here is an example of a linear congruence equation with two variables:

$$34x + 4y \equiv 3 \pmod{47}.$$

It might appear that the left-hand side is even and the right-hand side is odd. But in fact the right-hand side is really $3 + 47k$, which may be even if k is odd. Since $\gcd(4, 47) = 1$, one can write 1 as a combination of 4 and 47. For example, $1 = 4(12) - 47$. So, $4(12) \equiv 1 \pmod{47}$. If we multiply the original equation by 12, we obtain

$$12(34)x + 12(4)y \equiv 12(3) \pmod{47}.$$

Since $12(34) \equiv 12(-13) \equiv -156 + 3(47) \equiv -15 \pmod{47}$, this can be rewritten as

$$y \equiv 36 + 15x \pmod{47}.$$

Thus there are 47 solutions $\pmod{47}$, one for each choice of x.

2.6.3. Example. Now consider an equation of higher degree

$$x^2 + 1 \equiv 0 \pmod{65}.$$

With a little luck, you might notice that $x = 8$ is a solution. Following standard factorization techniques, you will be led to

$$(x - 8)(x + 8) \equiv x^2 - 64 \equiv x^2 + 1 \equiv 0 \pmod{65}.$$

If this were an exact equation over the integers or even the real numbers, you could conclude that $x = \pm 8$ were the only solutions. However, in solving this $\pmod{65}$, we are actually working in $\mathbb{Z}_{65}$. By Theorem 2.3.6, $\mathbb{Z}_{65}$ is

not an integral domain. The fact that it has zero divisors means that just because the product of $x-8$ and $x+8$ is 0 does not mean that either of these terms need be zero.

To deal with this problem, we use the Chinese Remainder Theorem but in reverse. The point is that the equation $x^2+1 \equiv 0 \pmod{65}$ has the same solutions as the system

$$\begin{aligned} x^2+1 &\equiv 0 \pmod 5 \\ x^2+1 &\equiv 0 \pmod{13} \end{aligned}$$

The advantage of this is that $\mathbb{Z}_5$ and $\mathbb{Z}_{13}$ are both fields. So

$$\begin{aligned} x^2+1 &\equiv (x-8)(x+8) \equiv 0 \pmod 5 \\ x^2+1 &\equiv (x-8)(x+8) \equiv 0 \pmod{13} \end{aligned}$$

do have exactly the obvious solutions. This is because in a field (or even in an integral domain) the product of two numbers is 0 only if one of the factors is 0. Thus we obtain the system

$$\begin{aligned} x &\equiv \pm 8 \pmod 5 \\ x &\equiv \pm 8 \pmod{13} \end{aligned}$$

This is really four sets of equations

$$\begin{aligned} x &\equiv 8 \pmod 5 \\ x &\equiv 8 \pmod{13} \end{aligned} \qquad \begin{aligned} x &\equiv -8 \pmod 5 \\ x &\equiv -8 \pmod{13} \end{aligned}$$

$$\begin{aligned} x &\equiv 8 \pmod 5 \\ x &\equiv -8 \pmod{13} \end{aligned} \qquad \begin{aligned} x &\equiv -8 \pmod 5 \\ x &\equiv 8 \pmod{13} \end{aligned}$$

Each of these sets of equations has a unique solution (mod 65) due to the Chinese Remainder Theorem again. The first two sets have the solutions $x \equiv \pm 8 \pmod{65}$ that we are already aware of. The last two sets have the solutions $x \equiv \pm 18 \pmod{65}$. So two surprising solutions turned up.

2.6.4. Example. Let us look at the problem of determining how many square roots of 1 there are modulo n. Working as above, we can factor n into a product of prime powers and solve a system of easier equations. Let us first solve the equation

$$x^2 - 1 \equiv 0 \pmod{p^d}$$

where p is prime. Now, x^2-1 factors as $(x-1)(x+1)$ so that $x = \pm 1$ are roots. Can there be any other roots? If there are, then $x-1$ and $x+1$ must both be divisible by some positive power of p. Hence p divides $\gcd(x-1, x+1)$, and thus divides $(x+1)-(x-1) = 2$. So when p is any *odd* prime, $x^2 - 1 \equiv 0 \pmod{p^d}$ has exactly two solutions, $x \equiv \pm 1 \pmod{p^d}$.

We must consider $p = 2$ separately. Following our argument above, we see that it may be possible that $2^a | x-1$ and $2^b | x+1$. The $\gcd(x-1, x+1)$ is at least $2^{\min\{a,b\}}$ and divides 2. Thus $\min\{a,b\} \leq 1$. The new solutions occur when $\min\{a,b\} = 1$, namely $a = 1$, $b = d-1$ or $a = d-1$, $b = 1$. This yields solutions

$$x \equiv 2^{d-1} \pm 1 \pmod{2^d}.$$

Hence $x^2 \equiv 1 \pmod{2^d}$ if and only if $x \equiv \pm 1 \pmod{2^{d-1}}$. Thus there are 4 solutions modulo 2^d if $d \geq 3$. By inspection, there is 1 solution modulo 2 and 2 solutions modulo 4.

To describe the number of solutions of $x^2 \equiv 1 \pmod{n}$, let us write the factorization of n as

$$n = 2^{d_0} p_1^{d_1} \dots p_k^{d_k},$$

where p_i are distinct odd primes and $d_i > 0$ for $i \geq 1$, but $d_0 = 0$ is allowed. Let $e = \max\{d_0 - 1, 0\}$. The problem reduces to solving the system

$$\begin{aligned} x &\equiv \pm 1 \pmod{2^e} \\ x &\equiv \pm 1 \pmod{p_1^{d_1}} \\ &\vdots \\ x &\equiv \pm 1 \pmod{p_k^{d_k}}. \end{aligned}$$

For each $i \geq 1$ there are two choices modulo $p_i^{d_i}$, and for $i = 0$, there are $s_0 = 1$,2 or 4 choices modulo 2^{d_0} depending on whether $d_0 - 2$ is negative, 0 or positive. Altogether this yields $s = 2^k s_0$ different systems of equations. By the Chinese Remainder Theorem, each system has a unique solution modulo n. So there are s square roots of 1 modulo n.

Unlike the case of real numbers, where it is not hard to solve degree 2 equations, solving quadratic equations in $\mathbb{Z}_n$ is a subject with considerable depth. Indeed, if p and q are odd primes, there is a surprising relationship between whether $x^2 \equiv p \pmod{q}$ is solvable and whether $x^2 \equiv q \pmod{p}$ is solvable. Known as Quadratic Reciprocity, this is a cornerstone result in Elementary Number Theory; see Section 3.6.

It is worth pointing out that our example of solving $x^2 - 1 \equiv 0 \pmod{65}$ illustrates another interesting phenomenon. We see

$$(x-8)(x+8) \equiv x^2 - 1 \equiv (x-18)(x+18) \pmod{65}.$$

We have therefore obtained two *different* factorizations of $x^2 - 1$ into "primes" (i.e. irreducible polynomials). This shows the failure of unique factorization for polynomials with coefficients in $\mathbb{Z}_{65}$.

Exercises

1. Find all solutions of $1713x \equiv 871 \pmod{2000}$.

2. Solve $64x \equiv 84 \pmod{66}$ completely.

3. Solve completely the equation $3x + 7y \equiv 11 \pmod{95}$.

4. Solve $x^2 \equiv 8x \pmod{437}$.

5. What are the cube roots of unity mod 91? In other words, solve the equation $x^3 - 1 \equiv 0 \pmod{91}$.

6. Solve $x^3 + x^2 + x + 1 \equiv 0 \pmod{91}$.

7. Solve the congruence system

$$\begin{aligned} 2x + 5y &\equiv 7 \pmod{82} \\ 7x + 13y &\equiv 10 \pmod{82}. \end{aligned}$$

2.7. Fermat's Little Theorem

The theorem to be proven in this section does not deserve the title 'little'. Indeed, it is a very important fact. However, Fermat's most famous non-theorem has so overshadowed all his other work that this lovely result is 'belittled'.

2.7.1 Fermat's Little Theorem. *Let p be a prime, and let a be an integer which is not a multiple of p. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Thus, $n^p \equiv n \pmod{p}$ for every integer n.

PROOF. Consider the function f mapping $\mathbb{Z}_p$ into itself used in the proof of Lemma 2.3.3:

$$f([x]) = [ax].$$

Since $\gcd(a, p) = 1$, this function is one-to-one and onto. We have $f([0]) = [0]$. So f gives a bijection of the non-zero elements of $\mathbb{Z}_p$. In other words, $\{[a], [2a], \ldots, [(p-1)a]\}$ is just the set $\{[1], [2], \ldots, [p-1]\}$ possibly in some other order. Hence

$$a(2a)(3a)\cdots((p-1)a) \equiv 1(2)(3)\cdots(p-1) \pmod{p}.$$

Simplifying both sides, we obtain

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}.$$

The element $[(p-1)!]$ is not zero (i.e. p does not divide $(p-1)!$), and since $\mathbb{Z}_p$ is a field, we can cancel out the $(p-1)!$ on each side of the equation. (Alternately, use Theorem 2.6.1 to justify the cancellation.) Thus,

$$a^{p-1} \equiv 1 \pmod{p}. \qquad \blacksquare$$

This can be reformulated as a result about $\mathbb{Z}_p$.

2.7.2. Corollary. *Let p be a prime. If $[a]$ is a non-zero element of $\mathbb{Z}_p$, then $[a]^{p-1} = [1]$. For all elements $[n]$, one has $[n]^p = [n]$.*

2.7.3. Corollary. *Let p be a prime. If $[a]$ is a non-zero element of $\mathbb{Z}_p$, then*

$$[a]^{-1} = [a]^{p-2}.$$

This theorem has many uses.

2.7.4. Example. One immediate use is in simplifying congruence equations. Very high powers can be replaced by lower ones. Consider the equation

$$x^{600}+29x^{543}-19x^{482}+199x^{301}+82x^{182}-75x^{121}+34x^{63}-60 \equiv 0 \pmod{61}.$$

It is immediately clear that $x \equiv 0 \pmod{61}$ is not a solution. For every other x, we have $x^{60} \equiv 1 \pmod{61}$. So the equation reduces to

$$1 + 29x^3 - 19x^2 + 199x + 82x^2 - 75x + 34x^3 - 60 \equiv 0 \pmod{61}.$$

This reduces to

$$2x^3 + 2x^2 + 2x + 2 \equiv 0 \pmod{61}.$$

After cancelling the 2 and pulling out the factor $x + 1$, this becomes

$$(x + 1)(x^2 + 1) \equiv 0 \pmod{61}.$$

Trial and error finds the solutions $x = \pm 11$. This means the cubic factors as

$$x^3 + x^2 + x + 1 \equiv (x + 1)(x - 11)(x + 11) \pmod{61}.$$

Since 61 is a prime, this is zero only if one of the three factors is zero. So the complete solution is $x \equiv 11$, 50 or 60 $\pmod{61}$.

The number $(p-1)!$ comes up in the proof of Fermat's Little Theorem. It is an interesting fact that $(p-1)! \pmod{p}$ can be computed.

2.7.5 Wilson's Theorem. *If p is a prime, $(p-1)! \equiv -1 \pmod{p}$.*

Proof. The result is trivial for $p = 2$. So without loss of generality, p is an odd prime. The idea is to evaluate the product $[1][2]\cdots[p-1]$ by pairing off each element $[a]$ with its inverse $[a]^{-1}$. There is a slight problem because $[a]$ might be its own inverse. This happens only if $[a]$ is root of $x^2 = [1]$, which factors as $(x - [1])(x + [1]) = [0]$. Since $\mathbb{Z}_p$ is a field, the only solutions are $[\pm 1]$.

Hence the non-zero elements pair off into $(p - 3)/2$ pairs of inverses $\{[a], [a]^{-1}\}$ and two singletons $[1]$ and $[-1]$. Multiplying together all the non-zero elements of $\mathbb{Z}_p$ results in a product of $(p-3)/2$ ones and $[1][-1] = [-1]$. That is, $(p-1)! \equiv -1 \pmod{p}$. ■

Exercises

1. Compute $2^{17^{15^{13}}} \pmod{13}$.

2. Find all solutions of

$$35x^{360} + 99x^{290} + 51x^{220} - 47x^{217} + 23x^{148} + 39x^{147} + 24x^{144} + 34x^{75} - 23x^{74} + 120x + 16 \equiv 0 \pmod{73}.$$

3. Solve $x^{39} + x^{25} + x^{14} + 1 \equiv 0 \pmod{91}$.

4. Suppose that p is a prime of the form $p = 4n+1$. Prove that $\pm(2n)!$ are roots of the equation $x^2 + 1 \equiv 0 \pmod{p}$.

5. Let $a > 1$ be any positive integer, and let p and q be primes. Show that if q divides $a^p - 1$, then $q \equiv 1 \pmod{p}$.

6. Use the previous exercise to test whether $2^{13} - 1$ and $2^{37} - 1$ are prime. This cuts down significantly on the number of prime divisors that need to be tested.

7. Suppose that n is the product of k distinct primes $p_1, \ldots, p_k$. Show that

$$\sum_{i=1}^{k} \left(\frac{n}{p_i}\right)^{p_i - 1} \equiv 1 \pmod{n}.$$

8.★ The Fermat numbers have the form $F_j = 2^{2^j} + 1$. The first few, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$, and $F_4 = 65537$ are prime. However, $F_5 = 641(6700417)$, and $p = 6700417$ is prime. Let

$$a = 2935363331541925531.$$

You may assume (correctly) that

$$a \equiv 1 \pmod{F_0F_1F_2F_3F_4p} \quad \text{and} \quad a \equiv -1 \pmod{641}.$$

Show that $2^k a + 1$ is never prime for $k \geq 1$.

9.★ Define a function f defined on $\{(n, m) : n, m \in \mathbb{N},\ n \geq 2\}$ as follows:

$$k = k(n, m) := (n-1)! + 1 - mn$$

$$f(n, m) := \frac{n-2}{2}\big(|k^2 - 1| - (k^2 - 1)\big) + 2.$$

Compute the range of f,

2.8. Euler's Theorem

In this section, we generalize Fermat's Little Theorem from primes to arbitrary integers. The problem is to figure out what the right generalization is. In order for $a^d \equiv 1 \pmod{n}$, it is necessary that $ax \equiv 1 \pmod{n}$ have a solution. By Theorem 2.6.1, this means that $\gcd(a, n) = 1$. It turns out

that this is also sufficient for some power of a to be congruent to 1 modulo n. In terms of the ring $\mathbb{Z}_n$, this is just the condition that $[a]$ has an inverse because $a(a^{d-1}) = 1$.

2.8.1. Definition. The Euler **totient** or **phi** function is the cardinality $\varphi(n)$ of $\mathbb{Z}_n^*$. That is, $\varphi(n)$ is the cardinality of

$$\{a : 1 \leq a \leq n,\ \gcd(a, n) = 1\}.$$

For example, $\varphi(12) = |\{1, 5, 7, 11\}| = 4$.

2.8.2. Example. If p is prime, it is clear that $\varphi(p) = p - 1$. More generally, if $n = p^d$, then $\gcd(a, n) \neq 1$ if and only if $p|a$. The multiples of p between 1 and n are given by $p, 2p, 3p, \ldots, p^d$, i.e. $p \cdot 1, p \cdot 2, \ldots, p \cdot (p^{d-1})$. We see there are p^{d-1} such numbers, so $\varphi(p^d) = p^d - p^{d-1} = p^{d-1}(p - 1)$. We will obtain a formula for an arbitrary $\varphi(n)$ in the next section.

You should notice that the proof of the following theorem is exactly the same as the proof of Fermat's Little Theorem.

2.8.3 Euler's Theorem. *If* $\gcd(a, n) = 1$*, then* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. Fix an integer a such that $\gcd(a, n) = 1$. Consider the function on $\mathbb{Z}_n$ given by $f([x]) = [ax]$. By Lemma 2.3.3, f is one-to-one and onto. As we have noted, if $[a]$ and $[x]$ are units, then so is $[ax]$. So, f maps $\mathbb{Z}_n^*$ onto itself. Multiplying all the units together yields the equation

$$\prod_{[x]\in\mathbb{Z}_n^*} [x] = \prod_{[x]\in\mathbb{Z}_n^*} [ax] = [a]^{\varphi(n)} \prod_{[x]\in\mathbb{Z}_n^*} [x].$$

Since $\prod_{[x]\in\mathbb{Z}_n^*}[x]$ is a unit, it can be cancelled off leaving

$$[a]^{\varphi(n)} = [1].$$

■

Exercises

1. If $\gcd(a, 561) = 1$, show that $a^{80} \equiv 1 \pmod{561}$. Calculate $\varphi(561)$.

2. Let $n = p_1p_2p_3$ be the product of three distinct primes. Let

$$d = \operatorname{lcm}\{p_1 - 1, p_2 - 1, p_3 - 1\}.$$

Prove that if $\gcd(a, n) = 1$, then $a^d \equiv 1 \pmod{n}$. Generalize.

3. (a) Suppose that n is the product of k distinct primes. Use the Chinese remainder theorem to show that if $m \equiv 1 \pmod{\varphi(n)}$, then $a^m \equiv a \pmod{n}$ for all integers a.
(b) Show by example that this is false for $n = 49$.

4. Before reading the next section, compute a few examples such as $\varphi(30)$, $\varphi(72)$, $\varphi(225)$ in order to conjecture a formula for $\varphi(n)$.

5.★ Compute $\prod_{[x]\in\mathbb{Z}_n^*}[x]$.
HINT: Use the information about square roots of 1 in $\mathbb{Z}_n$ to show that if n is odd with k distinct prime factors, then $\prod_{[x]\in\mathbb{Z}_n^*}[x] = [-1]^k$. Then find the general formula.

2.9. More on Euler's Phi Function

First we obtain a formula for $\varphi(n)$. The key tool is the Chinese Remainder Theorem.

2.9.1. Lemma. *If* $\gcd(n, m) = 1$, *then* $\varphi(nm) = \varphi(n)\varphi(m)$.

PROOF. It is clear that $\gcd(x, nm) = 1$ if and only if $\gcd(x, n) = 1$ and $\gcd(x, m) = 1$. Let

$$\mathcal{S}_n = \{a : 1 \le a \le n,\ \gcd(a, n) = 1\} \text{ and } \mathcal{S}_m = \{b : 1 \le b \le m,\ \gcd(b, m) = 1\}.$$

For each $a \in \mathcal{S}_n$ and $b \in \mathcal{S}_m$, consider the system

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

By the Chinese Remainder Theorem, this has a unique solution $\pmod{nm}$. Thus for each choice of $a \in \mathcal{S}_n$ and $b \in \mathcal{S}_m$, we obtain one element in $\mathcal{S}_{nm}$. Conversely, if $x \in \mathcal{S}_{nm}$, then $a \equiv x \pmod{n}$ belongs to $\mathcal{S}_n$ and $b \equiv x \pmod{m}$ belongs to $\mathcal{S}_m$. Thus,

$$\varphi(nm) = |\mathcal{S}_{nm}| = |\mathcal{S}_n||\mathcal{S}_m| = \varphi(n)\varphi(m).$$

■

2.9.2. Theorem. *If* $n = p_1^{d_1} \cdots p_k^{d_k}$ *where* p_i *are distinct primes, then*

$$\varphi(n) = n\big(1 - \tfrac{1}{p_1}\big) \cdots \big(1 - \tfrac{1}{p_k}\big).$$

Proof. We prove the result by induction on k. When $k = 1$, the number n is of the form $n = p^d$ where p is prime. Then Example 2.8.2 shows $\varphi(n) = p^{d-1}(p - 1) = n\big(1 - \frac{1}{p}\big)$.

For $k = 2$, the Lemma 2.9.1 applies directly to give

$$\begin{aligned}\varphi(p^d q^e) &= \varphi(p^d)\varphi(q^e)\\ &= p^d\big(1-\tfrac{1}{p}\big)q^e\big(1-\tfrac{1}{q}\big)\\ &= n\big(1-\tfrac{1}{p}\big)\big(1-\tfrac{1}{q}\big).\end{aligned}$$

Suppose that the result is true for $j < k$, and consider $n = p_1^{d_1}\cdots p_k^{d_k}$. Let $m = p_1^{d_1}\cdots p_{k-1}^{d_{k-1}}$. By hypothesis, $\varphi(m) = m\big(1-\frac{1}{p_1}\big)\cdots\big(1-\frac{1}{p_{k-1}}\big)$. Since $n = mp_k^{d_k}$ and $\gcd(m, p_k^{d_k}) = 1$, the lemma applies to show that

$$\begin{aligned}\varphi(n) &= \varphi(m)\varphi(p_k^{d_k})\\ &= m\big(1-\tfrac{1}{p_1}\big)\cdots\big(1-\tfrac{1}{p_{k-1}}\big)p_k^{d_k}\big(1-\tfrac{1}{p_k}\big)\\ &= n\big(1-\tfrac{1}{p_1}\big)\cdots\big(1-\tfrac{1}{p_k}\big).\end{aligned}$$

Therefore the theorem follows by induction. ■

The following result is a very useful property of the Euler phi function.

2.9.3. Theorem.

$$\sum_{d|n}\varphi(d) = n.$$

Proof. Let $\mathcal{S}_d = \{k : 1 \le k \le n,\ \gcd(k,n) = d\}$ for divisors d of n. Since the only possibilities for $\gcd(k,n)$ are divisors of n, it is clear that this provides a partition of $\{1,\dots,n\}$ into disjoint sets. Notice that if $k \in \mathcal{S}_d$, then $\gcd(k/d, n/d) = 1$ and $1 \le k/d \le n/d$. Conversely, if $\gcd(j, n/d) = 1$ and $1 \le j \le n/d$, then $k = jd$ belongs to $\mathcal{S}_d$. Hence there is a bijection between $\mathcal{S}_d$ and the units of $\mathbb{Z}_{n/d}$. So $|\mathcal{S}_d| = \varphi(n/d)$. Therefore

$$n = \sum_{d|n}|\mathcal{S}_d| = \sum_{d|n}\varphi\big(\tfrac{n}{d}\big).$$

Since $\frac{n}{d}$ runs over all of the divisors of n when d does, the desired formula follows. ■

Exercises

1. (a) Prove that if p is prime and n is divisible by p, then $\varphi(pn) = p\varphi(n)$.
(b) Show that in general if m divides n, the quantities $\varphi(nm)$ and $m\varphi(n)$ need not be equal.

2. Prove that for every positive integer k, there are only finitely many n for which $\varphi(n) = k$.

3. Find all n with $\varphi(n) = 12$.

4. (a) Prove there are infinitely many positive integers n with $\varphi(n) = \frac{n}{2}$.
(b) Prove that there are also infinitely many positive integers n with $\varphi(n) = \frac{n}{3}$.

5. Suppose that $\gcd(n, m) = 1$, and $d|nm$. Show that there is a *unique* factorization $d = ab$ so that $a|n$ and $b|m$.

6.★ Verify Theorem 2.9.3 directly for $n = p^k$. Then use Exercise 5 to prove it for products of distinct prime powers.

2.10. Primitive Roots

In this section, we show that for every prime p, one may always find an integer a such that $\{1, a, a^2, \ldots, a^{p-1}\}$ is a permutation of $\{1, 2, \ldots, p-1\}$ mod p. This is often useful, when one wishes to study problems that are multiplicative in nature, rather than additive.

2.10.1. Definition. If a is an element of $\mathbb{Z}_n^*$, its **order** is the smallest positive integer $d = \mathrm{ord}_n(a)$ such that $a^d \equiv 1 \pmod{n}$. Furthermore, say that a is a **primitive root** $\pmod{n}$ if the set of powers

$$\left\{a^k \pmod{n} : 1 \leq k \leq d\right\}$$

coincides with the set of all of $\mathbb{Z}_n^*$.

2.10.2. Proposition. *If $a^b \equiv a^c \equiv 1 \pmod{n}$, then $d = \gcd(b, c)$ satisfies $a^d \equiv 1 \pmod{n}$ also. Hence $a^b \equiv 1 \pmod{n}$ if and only if $\mathrm{ord}_n(a)|b$.*

Proof. By the Euclidean algorithm, there are integers s and t so that $d = bs + ct$. Hence

$$a^d \equiv \left(a^b\right)^s \left(a^c\right)^t \equiv 1 \pmod{n}.$$

In particular, $e = \gcd(b, \mathrm{ord}_n(a))$ satisfies $a^e \equiv 1 \pmod{n}$. Since $\mathrm{ord}_n(a)$ is the smallest such integer, and $e|\,\mathrm{ord}_n(a)$, we conclude that $e = \mathrm{ord}_n(a)$. Hence $\mathrm{ord}_n(a)|b$. ■

2.10.3. Corollary. *If $\gcd(a, n) = 1$, $\mathrm{ord}_n(a)|\varphi(n)$.*

Proof. By Euler's theorem, $a^{\varphi(n)} \equiv 1 \pmod{n}$. Hence by Proposition 2.10.2, $\mathrm{ord}_n(a)|\varphi(n)$. ■

The set of invertible elements $\mathbb{Z}_n^*$ of $\mathbb{Z}_n$ consists of the (equivalence classes of) elements relatively prime to n, and so has cardinality $\varphi(n)$. One sees that the powers of a belong to exactly $\mathrm{ord}_n(a)$ different classes $\pmod{n}$. For if $a^k \equiv a^l \pmod{n}$, with $k < l$, then $a^{l-k} \equiv 1 \pmod{n}$. Thus $\mathrm{ord}_n(a)|(l-k)$, and so $l > \mathrm{ord}_n(a)$. Conversely, if $\mathrm{ord}_n(a)|(l-k)$, it follows that $a^k \equiv a^l$

(mod n). So the distinct powers of a are precisely

$$\{a^k \pmod{n} : 1 \leq k \leq \mathrm{ord}_n(a)\}.$$

In particular, a is a primitive root of $\mathbb{Z}_n$ exactly when $\mathrm{ord}_n(a) = \varphi(n)$. So we obtain:

2.10.4. Proposition. *If* $\gcd(a, n) = 1$ *and* $\mathrm{ord}_n(a) = n - 1$, *then* n *is prime.*

When n is composite, there is frequently no primitive root. For example, modulo 15, the elements $\{2, 7, 8, 13\}$ have order 4, $\{4, 11, 14\}$ have order 2, and 1 has order 1. Since $\mathbb{Z}_{15}^*$ has 8 elements, there is no primitive root. However, for a prime p, it will be shown that a primitive root always exists. For example, modulo 17, the elements $\{3, 5, 6, 7, 10, 11, 12, 14\}$ are all primitive roots. The proof is based on a counting argument, and properties of the Euler phi function.

2.10.5. Lemma. *Let* p *be a prime. For each divisor* d *of* $p - 1$, *let* $f(d)$ *denote the number of elements of* $\mathbb{Z}_p^*$ *of order* d. *Then*

$$\sum_{e|d} f(e) = d$$

for every divisor d *of* $p - 1$.

Proof. By Fermat's Theorem, every element $a \in \mathbb{Z}_p^*$ satisfies $a^{p-1} = 1$. In other words, the congruence equation $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions modulo p. For each divisor d of $p-1$, one has that $\mathrm{ord}_p(a)|d$ if and only if $a^d \equiv 1 \pmod{p}$ (i.e. exactly when a is a root of $x^d - 1 \equiv 0 \pmod{p}$). Thus the number of roots is $\sum_{e|d} f(e)$. Also, one can factor

$$x^{p-1} - 1 \equiv (x^d - 1)p_d(x) \pmod{p}$$

where

$$p_d(x) = 1 + x^d + x^{2d} + \ldots + x^{p-1-d} = \sum_{0 \leq k < (p-1)/d} x^{kd}.$$

By Corollary 2.3.8, $p_d(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ distinct solutions modulo p, and $x^d - 1 \equiv 0 \pmod{p}$ has at most d solutions. But together, they have exactly $p-1$ distinct solutions. So both equations must have their full complement of solutions. In particular, $x^d \equiv 1 \pmod{p}$ had exactly d solutions modulo p. Therefore $\sum_{e|d} f(e) = d$. ■

Notice that by Theorem 2.9.3, the Euler phi function satisfies exactly the same set of equations as the function f of the lemma. That is the key to this theorem.

2.10.6. Theorem. *The function f of Lemma 2.10.5 coincides with the Euler phi function on the divisors of $p-1$. In particular, the field $\mathbb{Z}_p$ for p prime always has $\varphi(p-1)$ primitive roots. Therefore there is an element $a \in \mathbb{Z}_p^*$ so that the set of powers $\{a^k : 1 \le k \le p-1\}$ coincides with the set $\{1, 2, \ldots, p-1\}$ modulo p.*

Proof. We prove the result by induction on the size of the divisor d of $p-1$. For $d = 1$, there is, of course, exactly 1 solution of $x \equiv 1 \pmod{p}$. Thus

$$f(1) = 1 = \varphi(1).$$

Suppose that $f(e) = \varphi(e)$ for all divisors e of $p-1$ which are less than d. In particular, this is true for all divisors of d. Hence by the previous lemma and Theorem 2.9.3 ,

$$f(d) = d - \sum_{e|d,\ e<d} f(e) = d - \sum_{e|d,\ e<d} \varphi(e) = \varphi(d).$$

Therefore the number of primitive roots is $\varphi(p-1)$, which is non-zero. ■

There are many interesting unsolved questions concerning primitive roots. For example, in 1927, Artin conjectured that if $a \in \mathbb{Z}$ is not a perfect square and not -1, then there exist infinitely many primes p for which a is a primitive root in $\mathbb{Z}_p$. In particular, Artin's conjecture would imply that 2 is a primitive root in $\mathbb{Z}_p$ for infinitely many primes p. Currently, there is no value of a for which Artin's conjecture is known. In 1967, Hooley [**18**] did however give a conditional proof of Artin's conjecture assuming the generalized Riemann hypothesis. Unconditionally, Heath-Brown [**17**] proved in 1986 that at least one of 2, 3, or 5 must be a primitive root in $\mathbb{Z}_p$ for infinitely many primes p.

Now let us return to the problem of proving that a number p is definitely prime. By the previous discussion, it is sufficient to find some a with $\mathrm{ord}_p(a) = p-1$. However, it defeats the purpose if we must compute all $p-1$ powers. This is not necessary if $p-1$ can be factored. A method for factoring is described in the next section. It may be the case that $p-1$ has a lot of small factors. This will make factoring it substantially easier. The idea is this: factor $p-1 = \prod q_i^{d_i}$, then verify that $a^{p-1} \equiv 1 \pmod{p}$ and compute $a^{(p-1)/q_i} \pmod{p}$. If any of these is 1, then a is not a primitive root. But if they are all different from 1, then all powers of a up to $p-1$ are different, and a is a primitive root. Moreover, this shows that $\mathrm{ord}_p(a) = p-1$, so p is definitely prime. To see this, suppose that $a^k \equiv a^\ell \pmod{p}$ with $1 \le k < \ell < p$. Then if $m = \ell - k$, $a^m \equiv 1 \pmod{p}$. We also know that $a^{p-1} \equiv 1 \pmod{p}$. Let $d = \gcd(m, p-1)$. By Proposition 2.10.2, $a^d \equiv 1 \pmod{p}$. Clearly, d is a proper divisor of $p-1$. Thus d divides $(p-1)/q_i$ for some i, and so $a^{(p-1)/q_i} \equiv 1 \pmod{p}$.

2.10.7. Example. Consider the example $p = 113$. Factor $p - 1 = 112 = 2^4 7$. By hand, compute mod 113

$$\begin{array}{rcrcr} 2^7 & \equiv & 128 & \equiv & 15 \\ 2^{14} & \equiv & 225 & \equiv & -1 \\ 2^{28} & \equiv & 1 & & \end{array}$$

So 2 is not a primitive root. Try 3,

$$\begin{array}{rcrcr} 3^7 & \equiv & 2187 & \equiv & 40 \\ 3^{14} & \equiv & 1600 & \equiv & 18 \\ 3^{28} & \equiv & 324 & \equiv & -15 \\ 3^{56} & \equiv & 225 & \equiv & -1 \\ 3^{112} & \equiv & 1 & & \end{array}$$

So 3 is looking good so far.

$$\begin{array}{rcrcr} 3^8 & \equiv & 120 & \equiv & 7 \\ 3^{16} & \equiv & 49 & & \end{array}$$

Thus we see that $3^{112} \equiv 1 \pmod{113}$, and $3^{56} \not\equiv 1 \pmod{113}$, and $3^{16} \not\equiv 1 \pmod{113}$. So 3 is a primitive root, and 113 is prime.

Of course, this method is not interesting for such small numbers. Try some of the following exercises with a symbolic computation program.

Exercises

1. Show that 19 is a primitive root for $p = 191$.

2. Show that 2 is a primitive root for $p = 2549$.

3. Let p be prime and let $a \in \mathbb{Z}$ be a primitive root mod p. Prove that a is a primitive root mod p^2 if and only if $a^{p-1} \not\equiv 1 \pmod{p^2}$.

4. Let $p \neq q$ be odd primes. Prove that there are no primitive roots mod pq.

5. Let p, q, r be pairwise distinct primes which are not necessarily odd. Prove that there are no primitive roots mod pqr.

6. Find a primitive element of $\mathbb{Z}^*_{27943}$. Give a short list of congruences that prove that it is a primitive root, and hence that 27943 is prime. You can use computer software.

7. Find a primitive root for $p = 1423554023$ using computer software. Give a short list of congruences that prove that it is a primitive root, and hence that p is prime.

Notes on Chapter 2

Linear Diophantine equations were discussed by the Greek mathematician Diophantus in the 3rd century CE, though he did not have a complete solution. The Hindu school in India studied these equations in the 6th and 7th century CE, and Brahmegupta had a method for finding a solution. It was in the 16th and 17th centuries that the Europeans wrote about it. Euler gave a complete solution in the modern style in 1734. It was Gauss who introduced the modern notation of congruence modulo n.

The abstract notion of a ring was given by Fraenkel in 1914 and extended by Sono in 1917. However many concrete examples such as $\mathbb{Z}_n$ were well known much earlier. The first non-commutative example was the ring of quaternions due to Hamilton in 1843. Cayley considered the space of $n \times n$ matrices as a ring in 1855. See [**19**] for more on this history.

The Chinese remainder problem, as the name suggests, first arose in Chinese writings from the first century CE. The Greek and the Indian schools also studied this problem. A complete solution was provided by Yih-hing in 717 CE. The Arab school has writings on it from about 1000 CE. The Italians wrote about partial solutions in the late 12th century. A German manuscript from the 15th century produced the same solution as Yih-hing. The modern solution in complete generality was given by Euler, and also Gauss, in the mid-18th century.

Fermat's little theorem was stated by Fermat in 1640. Euler gave a proof of it in 1736, and the generalization to Euler's theorem in 1760.

Much information about this history can be found in the volume by Dickson [**9**, Vol.II]. Kleiner [**20**] is another source worth reading. Cooke [**8**] contains a lot of information of mathematics before the modern era.

See Hardy and Wright [**15**] for all of this material and many extensions, plus many historical notes. Stark [**37**] is also an excellent source for this material.

Chapter 3

Diophantine Equations and Quadratic Number Domains

Diophantine equations refer to equations or systems of equations in which both the coefficients and the unknowns are integers. Generally, there are more unknowns than equations. But since we are interested in integer solutions, it is often difficult to decide if there are any solutions at all. The most famous Diophantine equation is Fermat's equation

$$x^n + y^n = z^n$$

for $n \geq 3$. Fermat wrote in the pages of a book (circa 1637) that he had a truly marvelous proof that there are no solutions, but it was too long to fit in the margin. However, there is no way to know for certain if he really had such a proof. Fermat never published anything in mathematics, nor did he often communicate his methods to others. It is revealing, however, that he wrote to others that he had a proof for the case $n = 4$, but never claimed to have a general proof in his correspondence.

Euler solved the case $n = 3$ in 1770. Legendre and Dirichlet independently solved the case $n = 5$ around 1825. Sophie Germain was a self-taught French mathematician in the late 18th century, a time when women were not welcomed into academic circles. She corresponded with Lagrange, Legendre and Gauss under a pseudonym. She did some important work on Fermat's problem which was unpublished, but was mentioned by Legendre. Some of her results were still being reproved by others in the 20th century.

The early development of abstract algebra, especially rings and fields, was in part motivated by an attempt to solve Fermat's problem. Several 'proofs' were found to be incorrect because they falsely assumed unique factorization in certain number domains. Kummer was the first to provide a solution for infinitely many primes in 1847, based on an analysis of the failure of unique factorization. His proof works for *regular primes*, which includes all primes less than 100 except 37, 59 and 67.

Exciting news reached the mathematical community in June 1993 when Andrew Wiles announced the final dramatic step to the solution of this 350-year-old problem at a conference in Cambridge. The statement of his actual results do not immediately look like they apply to Fermat's question, as they refer to some advanced notions about elliptic curves. Indeed, his results are much more far reaching than a single equation such as Fermat's. It turned out that there was a gap in part of his proof. He and Richard Taylor worked on the gap and eventually completed the argument. In particular, these results combine with known work to finally resolve the most famous mathematical conundrum of our time.

In this chapter, we will look at a few special cases of Diophantine equations, and will see a variety of techniques for solving them. We also will take an excursion into some other number systems to see that the theorems we proved in the last chapter are indeed special. The quadratic number domains have a nice theory which imitates, yet varies from, the integers. Several of these domains have applications to the number theory of the integers themselves. We finish the chapter with a proof of Gauss's famous Law of Quadratic Reciprocity, which allows one to calculate whether a number a is a square modulo a prime p.

3.1. Pythagorean Triples

In this section, we will study the well known problem of determining all of the integer solutions of the Pythagorean equation

$$x^2 + y^2 = z^2.$$

Of course, if (x, y, z) is a solution, then (ax, ay, az) is also a solution. So it is natural to insist that $\gcd(x, y, z) = 1$. Of course, any integer which divides any two of x, y, z divides the third as well. So, it suffices to say $\gcd(x, y) = 1$.

We will give two characterizations of such (x, y, z). The first uses an algebraic approach, while the second uses a geometric method.

Algebraic approach. The first observation is obtained by looking at squares of odd and even numbers. All such squares are congruent to 0 and 1 modulo 4 respectively. Thus the sum of two odd squares is congruent to 2 (mod 4), and no square has this form. Since we have ruled out the case of x and y both being even by assuming that they are relatively prime, it follows that one, say x, is even, and the other, y, is odd. Hence, z is also odd.

Now consider the equation

$$x^2 = z^2 - y^2 = (z + y)(z - y).$$

Since x, $z+y$, and $z-y$ are all even, there are positive integers a, b, c so that

$$x = 2a, \qquad z + y = 2b \quad \text{and} \quad z - y = 2c.$$

Our equation becomes

$$4a^2 = 4bc \quad \text{or} \quad a^2 = bc.$$

Now $\gcd(b, c)$ divides $\gcd(b + c, b - c) = \gcd(z, y) = 1$. Thus b and c are relatively prime. But bc is a perfect square, meaning each prime factor occurs an even number of times. As b and c have no common factors, they must both be squares. Let u and v be positive integers such that $b = u^2$ and $c = v^2$, and thus $a = uv$. Substituting back in yields

$$x = 2uv \qquad y = u^2 - v^2 \qquad z = u^2 + v^2.$$

Furthermore, $\gcd(u, v) = \sqrt{\gcd(b, c)} = 1$. Since y is odd, exactly one of u and v is odd.

On the other hand, if $u > v$ are relatively prime, one even and one odd, then $x = 2uv$, $y = u^2 - v^2$ and $z = u^2 + v^2$ are relatively prime, and satisfy

$$x^2 + y^2 = 4u^2v^2 + u^4 - 2u^2v^2 + v^4 = u^4 + 2u^2v^2 + v^4 = z^2.$$

This solves the problem completely.

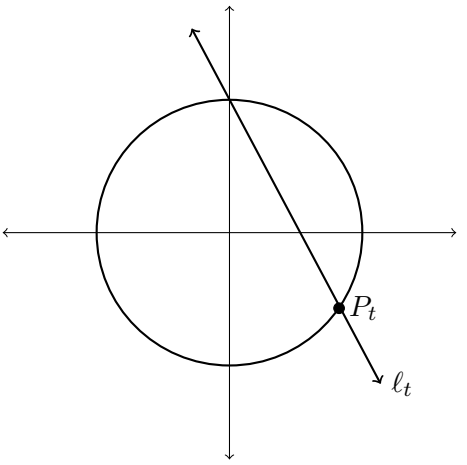
For the general solution of Pythagorean triples, one must put the common factors back in. So the most general solution is given by

$$x = 2kuv \qquad y = k(u^2 - v^2) \qquad z = k(u^2 + v^2)$$

for arbitrary integers u, v, and k. Note however that to get $\gcd(x, y) = k$, we need to specify that exactly one of u, v is even and $\gcd(u, v) = 1$.

Geometric approach. Observe that (x, y, z) is a solution if and only if the point (ax, ay, az) is a rational solution for all $a \neq 0$ in $\mathbb{Q}$. If we take $a = \frac{1}{z}$, we obtain a rational solution $\left(\frac{x}{z}, \frac{y}{z}, 1\right)$. Conversely, if $(x, y, 1)$ is a rational solution, then clearing the denominator yields integer solutions. Therefore, it is enough to classify $(x, y) \in \mathbb{Q}^2$ with $x^2 + y^2 = 1$. We see that $Q = (0, 1)$ is such a solution.

Consider the line ℓ_t through $(0,1)$ with slope t, and let P_t be the intersection of ℓ_t with the circle $x^2+y^2=1$.



Let's express P_t in terms of t. The line ℓ_t is given by $y=tx+1$. Substituting this expression for y into $x^2+y^2=1$, we find

$$1 = x^2 + (tx+1)^2 = (t^2+1)x^2 + 2tx + 1.$$

The two solutions to this equation are $x=0$ and

$$x = -\frac{2t}{t^2+1}. \tag{3.1.1}$$

Plugging back into $y=tx+1$, we have

$$y = tx + 1 = \frac{1-t^2}{t^2+1}. \tag{3.1.2}$$

Therefore,

$$P_t = \Big(-\frac{2t}{t^2+1}, \frac{1-t^2}{t^2+1} \Big).$$

Notice that if $t \in \mathbb{Q}$, then $P_t \in \mathbb{Q}^2$. Conversely, suppose $P_t \in \mathbb{Q}^2$ and $P_t \neq (0,1)$. Then since t is the slope of the line between P_t and $(0,1)$, we see $t \in \mathbb{Q}$. Hence, we have shown

$$\begin{aligned}\{(x,y) \in \mathbb{Q}^2 : x^2+y^2=1\} &= \{P_t : t \in \mathbb{Q}\} \cup \{(0,1)\} \\ &= \Big\{ \Big(-\frac{2t}{t^2+1}, \frac{1-t^2}{t^2+1} \Big) : t \in \mathbb{Q} \Big\}.\end{aligned}$$

Note that setting $t=0$ yields the point $(0,1)$.

Now, set $t = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ relatively prime and $b \neq 0$. Then

$$1 = \Big(\frac{-2t}{t^2+1}\Big)^2 + \Big(\frac{1-t^2}{t^2+1}\Big)^2 = \Big(\frac{2ab}{a^2+b^2}\Big)^2 + \Big(\frac{a^2-b^2}{a^2+b^2}\Big)^2.$$

Multiplying through by a^2+b^2, we see that all of the integer solutions of $x^2+y^2=z^2$ (up to scalar) are given by

$$(2ab, a^2-b^2, a^2+b^2).$$

The key geometric trick which made this argument work was to find one rational solution Q of $x^2 + y^2 = 1$ and then parameterize all other solutions by intersecting our equation with a rationally sloped line through Q. The reader may wonder if Diophantine equations other than $x^2 + y^2 = z^2$ may also be solved using this method. This question forms part of a beautiful subject known as Arithmetic Geometry. Equations of degree 3 in x, y, z are objects known as elliptic curves; rational points on elliptic curves is a subject of active research and has deep connections to the Fermat equation mentioned at the beginning of this chapter. For equations of degree at least 4 in x, y, z, a theorem of Faltings shows that there are only finitely many rational solutions. Faltings was awarded the Fields Medal for his seminal work on this subject.

Exercises

1. Show that there are infinitely many relatively prime solutions of

$$x^2 + y^2 = z^4.$$

2. Find all solutions of $x^2 + 3y^2 = z^2$.

3. Find all relatively prime solutions of $x^2 + 2y^2 = z^2$.

4. Use point $Q = (1, 1)$ to find all rational points on the circle $x^2 + y^2 = 2$.

5. Solve the Diophantine equation $x^2 + 44^2 = z^6$.

3.2. Fermat's Equation for $n = 4$

The complete solution of the Pythagorean triple problem allows us to analyze the Diophantine equation

$$x^4 + y^4 = z^2.$$

It will be shown that this has no solutions. Hence the Fermat equation

$$x^4 + y^4 = z^4$$

has no solutions either.

The method of proof is called Fermat's method of **infinite descent**. The basic idea is to start with the smallest possible solution (*if it exists*), meaning that z is as small as possible. Then using the given solution, construct a *smaller* solution. Of course, this is a contradiction which implies that the assumption that there were any solutions at all was wrong. This is called infinite descent because one can construct an infinite sequence of smaller and smaller solutions, which is not possible.

3.2.1. Theorem. *The equation $x^4 + y^4 = z^2$ has no positive integer solutions.*

Proof. So, let us assume that there are solutions of $x^4+y^4=z^2$ in positive integers. Among all solutions, we choose x,y and z so that z is minimal. In particular, $\gcd(x,y)=1$. Since x^2, y^2, and z is a Pythagorean triple, there are relatively prime positive integers u and v such that

$$x^2=2uv \qquad y^2=u^2-v^2 \qquad z=u^2+v^2.$$

(It may be necessary to interchange x and y so that x is even, and y is odd.)

This produces another Pythagorean triple $v^2+y^2=u^2$. Thus, v must be even, as y is odd. Consider the equation $x^2=(2v)u$. As $\gcd(u,2v)=1$, it follows that u and $2v$ are squares. Hence there are positive integers a and b so that $u=a^2$ and $v=2b^2$.

Using the solution for Pythagorean triple system $v^2+y^2=u^2$, we obtain relatively prime positive integers c and d so that

$$v=2cd \qquad y=c^2-d^2 \qquad u=c^2+d^2.$$

Hence, $b^2=cd$ and $a^2=c^2+d^2$. Once again, since $b^2=cd$ and $\gcd(c,d)=1$, it follows that c and d are perfect squares, say $c=m^2$ and $d=n^2$. Substituting back in yields

$$m^4+n^4=a^2.$$

Finally, $a\le a^2=u<u^2+v^2=z$.

So, we have succeeded in producing a smaller solution of our equation, contrary to the hypothesis that we started with the smallest one. This must imply that there are no solutions at all. ■

Exercises

1. Show that there are no positive integer solutions to $x^4+4y^4=z^2$.

2. Show that there are no positive integer solutions to $x^4-y^4=z^2$.

3. Show that there is no right angle triangle with sides of integer lengths whose area is a perfect square.

4. Solve $x^2+12=y^4$ for $x,y\in\mathbb{N}$.

5. Show that if $x,y,p\in\mathbb{N}$ with p is prime and $x^3+y^3=p$, then $p=2$. What changes if we allow $x,y\in\mathbb{Z}$? Find a few solutions.

6. Find all integer solutions of $x^2-11y^2=3$.
HINT: solve it mod 3 first.

7. Find all integer solutions of $x^4+y^4=13z^4$.
HINT: try to solve it modulo some primes.

3.3. Quadratic Number Domains

A number d is called *square free* if it has no repeated prime factor. Let d be a square free integer (except 1). Define

$$\mathbb{Z}[\sqrt{d}] = \{n + m\sqrt{d} : n, m \in \mathbb{Z}\}.$$

One may check directly that this set is closed under addition and multiplication; and thus is a commutative ring. It also has the important property

$$\text{if } x, y \in \mathbb{Z}[\sqrt{d}] \text{ and } xy = 0 \quad \text{then} \quad x = 0 \text{ or } y = 0.$$

This follows since $\mathbb{Z}[\sqrt{d}]$ is contained in the real numbers $\mathbb{R}$ (when $d > 0$) or the complex numbers $\mathbb{C}$ (when $d < 0$), both of which have this property. In other words, $\mathbb{Z}[\sqrt{d}]$ is an integral domain.

In fact, $\mathbb{Z}[\sqrt{d}]$ sits inside a smaller field

$$\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} : r, s \in \mathbb{Q}\}.$$

One checks that $\mathbb{Q}[\sqrt{d}]$ is an integral domain. To see that non-zero elements have inverses, notice that

$$\left(r + s\sqrt{d}\right) \frac{r - s\sqrt{d}}{r^2 - ds^2} = 1.$$

It is a simple exercise based on the irrationality of $\sqrt{d}$ to see that

$$r + s\sqrt{d} = a + b\sqrt{d}$$

implies that $a = r$ and $b = s$ for all rational numbers a, b, r and s. In particular, $r^2 - ds^2 \neq 0$ unless $r = s = 0$. Now we will introduce an important function which will make computations possible.

3.3.1. Definition. For $x = r + s\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, define the **conjugate** of x to be $\tilde{x} = r - s\sqrt{d}$. Let the **norm** of x be $N(x) = x\tilde{x} = r^2 - ds^2$.

Note that if $x \in \mathbb{Q}[\sqrt{d}]$, then $N(x)$ is rational. If $x \in \mathbb{Z}[\sqrt{d}]$, then $N(x)$ is an integer.

3.3.2. Lemma. *For $x, y \in \mathbb{Q}[\sqrt{d}]$,*

(1) $\widetilde{x+y} = \tilde{x} + \tilde{y}$.
(2) $\widetilde{xy} = \tilde{x}\tilde{y}$.
(3) $N(xy) = N(x)N(y)$.
(4) $N(x) = 0$ *if and only if* $x = 0$.

Proof. The proof consists of straightforward computations, and will be left to the exercises. ■

Recall from Definition 1.8.3 that a unit x of a commutative ring R is an element with an inverse y, i.e., $xy = 1$. In $\mathbb{Z}[\sqrt{2}]$, a simple calculation shows that

$$(17 + 12\sqrt{2})(17 - 12\sqrt{2}) = 1.$$

So $17 + 12\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. We need a criterion to decide when something is a unit.

3.3.3. Proposition. *An element $x \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $N(x) = \pm 1$.*

Proof. If $xy = 1$, then $N(x)N(y) = N(1) = 1$. But $N(x)$ and $N(y)$ are integers, so they are both ± 1. Conversely, if $N(x) = \pm 1$, $y = N(x)\tilde{x}$ satisfies $xy = N(x)^2 = 1$. So x is a unit. ■

This proposition shows that the units if $\mathbb{Z}[\sqrt{d}]$ correspond exactly to integer solutions of **Pell's equation**

$$n^2 - dm^2 = \pm 1.$$

When d is positive, there are always infinitely many solutions. We will look at a few special cases in the next section. When $d \leq -2$, only ± 1 are units. The case $d = -1$ is special. See section 3.5.

3.3.4. Definition. In a quadratic number domain, an element x is called a **prime** if (i) x is not a unit, and (ii) whenever x factors as $x = ab$, either a or b is a unit.

3.3.5. Remark. Notice that this definition is a special case of the one given in Definition 1.8.6. For rings more general than quadratic number domains, the term "irreducible" is used instead of "prime."

One can factor 2 in $\mathbb{Z}$ as

$$2 = (1)(2) = (2)(1) = (-1)(-2) = (-2)(-1).$$

We consider these to be trivial factorizations because one factor is always a unit. The primes in $\mathbb{Z}$ by this definition are just the ordinary primes and their negatives.

The following lemma gives us a simple test for primes. However, the converse is not true; so be careful how you use it.

3.3.6. Lemma. *If $N(x)$ is prime, then x is a prime.*

Proof. If $x = ab$, then $N(x) = N(a)N(b)$. If $N(x)$ is prime, then either $N(a)$ or $N(b)$ equals ± 1. Hence either a or b is a unit by Proposition 3.3.3. Therefore x is prime. ■

3.3.7. Example. Consider $\mathbb{Z}[\sqrt{2}]$ again. Since $N(2+\sqrt{2}) = 2$ is prime, $2+\sqrt{2}$ is a prime. The number 2 itself is *not* prime! It factors as $2 = \sqrt{2}\sqrt{2}$, and $N(\sqrt{2}) = -2 \neq \pm 1$. Also 7 is not prime because $7 = (3-\sqrt{2})(3+\sqrt{2})$.

The integer 5 *is* prime in $\mathbb{Z}[\sqrt{2}]$, even though $N(5) = 25$ is not prime. If 5 were not prime, it would factor as $5 = xy$, where neither x nor y is a unit. Then $25 = N(5) = N(x)N(y)$. Since x and y are not units, neither $N(x)$ nor $N(y)$ equals ± 1. Thus, one must have $N(x) = N(y) = \pm 5$. Let us write $x = n + m\sqrt{2}$. Then

$$n^2 - 2m^2 = \pm 5.$$

This is impossible. To see this, consider this equation modulo 5. One obtains

$$n^2 \equiv 2m^2 \pmod 5.$$

However, the squares modulo 5 are congruent to 0, 1 or 4. Thus the only solution occurs when

$$n \equiv m \equiv 0 \pmod 5.$$

Thus the only way that $n^2 - 2m^2$ can be a multiple of 5 is if both n and m are multiples of 5. Then $n^2 - 2m^2$ is a multiple of 25; and so never equals ± 5. We conclude that 5 is prime in $\mathbb{Z}[\sqrt{2}]$.

Let us show that every element of $\mathbb{Z}[\sqrt{d}]$ has at least one factorization into primes. Later, we will discuss what unique factorization should mean.

3.3.8. Lemma. *Every non-zero element of $\mathbb{Z}[\sqrt{d}]$ factors as the product of a unit and finitely many primes.*

Proof. The proof is basically the same as the proof we gave for the integers. The size of elements of $\mathbb{Z}[\sqrt{d}]$ will be measured by the norm function.

Consider the set

$$S = \{x \in \mathbb{Z}[\sqrt{d}] : x \text{ does not factor as a finite product of primes}\}.$$

If this set is empty, the lemma is true. Otherwise, the set

$$\{|N(x)| : x \in S\}$$

has a smallest element. Let x be an element of S for which $|N(x)|$ is as small as possible. If x were prime, it would factor as the product of one prime and so would not belong to S. Hence x factors as $x = ab$ so that $|N(a)| < |N(x)|$ and $|N(b)| < |N(x)|$. Therefore, both a and b must factor as products of primes, say

$$a = up_1 \dots p_k \quad \text{and} \quad b = vq_1 \dots q_l,$$

where u and v are units and p_i and q_j are all primes. But then

$$x = (uv)p_1 \dots p_k q_1 \dots q_l$$

is the desired factorization of x. This contradicts the fact that x belongs to S. We conclude that S is empty and the lemma is true. ■

What does unique factorization mean in this context? Consider

$$11 = (5\sqrt{3}+8)(5\sqrt{3}-8) = (2\sqrt{3}-1)(2\sqrt{3}+1).$$

Notice that

$$N(5\sqrt{3}\pm 8) = N(2\sqrt{3}\pm 1) = 11.$$

So the factors are prime. Are they really two different factorizations of 11 in $\mathbb{Z}[\sqrt{3}]$? No, they're not. Notice that $2-\sqrt{3}$ is a unit with inverse $2+\sqrt{3}$. Now

$$(5\sqrt{3}+8)(2-\sqrt{3}) = 2\sqrt{3}+1.$$

So these two primes are in the same relationship here as ± 5 are in $\mathbb{Z}$. Two primes p and q are called **associates** if there is a unit u such that $q = up$. So we can compute

$$\begin{aligned} 11 &= (5\sqrt{3}+8)(5\sqrt{3}-8) \\ &= \big((5\sqrt{3}+8)(2-\sqrt{3})\big)\big((2+\sqrt{3})(5\sqrt{3}-8)\big) \\ &= (2\sqrt{3}+1)(2\sqrt{3}-1) \\ &= (2\sqrt{3}-1)(2\sqrt{3}+1). \end{aligned}$$

These two factorizations are essentially the same because the only difference is obtained by multiplying primes by units, and permuting the factors.

On the other hand, consider the following situation in $\mathbb{Z}[\sqrt{10}]$.

$$6 = (2)(3) = (4+\sqrt{10})(4-\sqrt{10}).$$

We compute that $N(2) = 4$, $N(3) = 9$, and $N(4\pm\sqrt{10}) = 6$. If these numbers factor non-trivially in $\mathbb{Z}[\sqrt{10}]$, then there would be elements $x = n + m\sqrt{10}$ with $N(x) = n^2 - 10m^2 = \pm 2$ and $N(x) = \pm 3$. However, reducing modulo 10, this requires that $n^2 \equiv 2, 3, 7$ or $8 \pmod{10}$. But a perfect square is congruent to 0, 1, 4, 5, 6, or 9 $\pmod{10}$. Therefore 2, 3 and $4\pm\sqrt{10}$ are primes in $\mathbb{Z}[\sqrt{10}]$. Neither 2 nor 3 is an associate of $4\pm\sqrt{10}$ because their norms are different. So the domain $\mathbb{Z}[\sqrt{10}]$ does not have the unique factorization property.

A domain in which every element has exactly one factorization into primes up to permutations and multiplication by units is called a **Unique Factorization Domain** or **UFD**. The key is the analogue of Lemma 1.6.1. Some of these domains have a Euclidean algorithm, which is easily deduced if there is a division algorithm. See Section 1.8 for an introduction to these ideas. Try it out with $x = 2$ and $y = 4+\sqrt{10}$ to see that this does not hold in $\mathbb{Z}[\sqrt{10}]$. It is an interesting and difficult problem in number theory to determine which quadratic number domains are Euclidean, and which are UFD's. There are only finitely many Euclidean domains. There are more UFD's, and it is conjectured that there are infinitely many of them.

The interested reader should consult a book on number theory to get more information. We recommend Stark [**37**].

There is one more subtle point. The ring $\mathbb{Z}[\sqrt{5}]$ is not a UFD. To see this, notice that $4 = (\sqrt{5}+1)(\sqrt{5}-1) = (2)(2)$. Also, all the factors have norm 4. We see that $n^2 - 5m^2 = 2$ has no solutions by looking at this equation mod 5. Clearly, 2 and $\sqrt{5}+1$ are not associates. Thus factorization is not unique in $\mathbb{Z}[\sqrt{5}]$. However, in this case, the reason is that we left some important elements out of our ring. All the numbers $x = n + m\sqrt{5}$ satisfy a monic quadratic equation with integer coefficients, namely

$$X^2 - 2nX + (n^2 - 5m^2) = 0.$$

However, the element $(1 + \sqrt{5})/2$ belongs to $\mathbb{Q}[\sqrt{5}]$, and is a root of $X^2 - X - 1$. The collection of all numbers in $\mathbb{Q}[\sqrt{5}]$ satisfying such an equation turns out to be all numbers of the form $(n + m\sqrt{5})/2$ where n and m are integers such that $n \equiv m \pmod 2$. In this case, $N(x) = \frac{n^2-5m^2}{4} \in \mathbb{Z}$. In the larger ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, there are the units $(1 \pm \sqrt{5})/2$. It is known as the ring of integers in $\mathbb{Q}[\sqrt{5}]$ because this is the set of all elements in $\mathbb{Q}[\sqrt{5}]$ with integer norm. Now 2 and $1 \pm \sqrt{5}$ are associates in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. In fact, $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a Euclidean Domain.

It can be shown that the ring of integers in $\mathbb{Q}[\sqrt{d}]$ is $\mathbb{Z}[\sqrt{d}]$ when $d \not\equiv 1 \pmod 4$, and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ when $d \equiv 1 \pmod 4$. Moreover, when $d \equiv 1 \pmod 4$, $\mathbb{Z}[\sqrt{d}]$ can never be a UFD. To see this, let $d = 4k+1$. Notice that

$$2|4k = (1 + \sqrt{d})(-1 + \sqrt{d}).$$

We claim that 2 is prime in $\mathbb{Z}[\sqrt{d}]$. It has norm $N(2) = 4$, so any proper factor must have norm ± 2. Consider the equation

$$\pm 2 = n^2 - dm^2 \equiv n^2 - m^2 \pmod 4.$$

The left-hand side is congruent to 2 (mod 4), which can never be the difference of two squares. Now the prime 2 divides $(1 + \sqrt{d})(-1 + \sqrt{d})$, but does not divide either $\pm 1 + \sqrt{d}$. So there is no unique factorization.

The list of the rings of integers of $\mathbb{Q}[\sqrt{d}]$ which are Euclidean domains with respect to the norm function is finite: $d =$

$$-11,\ -7,\ -3,\ -2,\ -1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73.$$

The list of Euclidean domains for some other function includes $d = 14$, and may be infinite. The list of UFDs is larger, and is almost surely infinite. The negative values of d are all known though, and there are only finitely many. In addition to the norm Euclidean domains, there are -163, -67, -43, -19. The additional positive ones with $d < 100$ are

$$14,\ 22,\ 23,\ 31,\ 38,\ 43,\ 46,\ 47,\ 53,\ 59,\ 61,\ 62,\ 71,\ 77,\ 83,\ 86,\ 89,\ 93,\ 94,\ 97.$$

Exercises

1. Show that $n + m\sqrt{d} = k + l\sqrt{d}$ for $k, l, m, n \in \mathbb{Q}$ implies that $k = n$ and $l = m$.

2. Verify Lemma 3.3.2.

3. (a) Show that 2 and 3 are not prime in $\mathbb{Z}[\sqrt{3}]$.
(b) Show that $5 - 2\sqrt{3}$ is prime in $\mathbb{Z}[\sqrt{3}]$.
(c) Show that 5 is prime in $\mathbb{Z}[\sqrt{3}]$.

4. Show that there is no division algorithm for $\mathbb{Z}[\sqrt{10}]$ with $f(x) = |N(x)|$ by showing that any remainder on dividing $4 + \sqrt{10}$ by 2 has norm with absolute value at least 6.
HINT: consider the norm of the remainder modulo 20.

5. Show that there are infinitely many integer solutions of $n^2 - 3m^2 = 1$. Find an explicit recursion formula that generates your set of solutions.

6. Show that $n^2 - 5m^2 = 2$ has no solutions.

3.4. Pell's Equation

The units (invertible elements) of $\mathbb{Z}[\sqrt{d}]$ are of the form $x + y\sqrt{d}$ such that

$$x^2 - dy^2 = \pm 1.$$

For d positive, one might suspect that there are non-trivial solutions. In fact, there are always infinitely many solutions for every positive square free d. The proof of this is beyond the scope of this book. If you are interested, consult [**37**]. The proof is based on the theory of continued fractions. Brute force is not likely to succeed with this problem because some fairly small numbers have very large smallest solutions. For example, for $d = 109$, the smallest solution is

$$x = 158\,070\,671\,986\,249 \qquad y = 15\,140\,424\,455\,100.$$

This problem has a long history, and it was completely solved in 1150 by Bhaskara. Fermat solved it for $d \leq 150$ and challenged a group of British mathematicians to solve certain larger numbers. This was done by Broukner, but later falsely attributed to Pell by Euler. It seems that Pell was not responsible for either the problem or its solution, but his name has stuck.

In this section, we will solve the special case

$$x^2 - 5y^2 = \pm 1.$$

We see $x = 2$ and $y = 1$ gives a non-trivial solution. This means that $2 + \sqrt{5}$ is a unit in $\mathbb{Z}[\sqrt{5}]$ of norm -1. Thus any power of it is a unit (with norms alternating ± 1). That is, the pairs $\{\pm x_n, \pm y_n\}$ obtained from

$$x_n + y_n\sqrt{5} = (2 + \sqrt{5})^n$$

are solutions. The even pairs $\{\pm x_{2n}, \pm y_{2n}\}$ are solutions of $x^2 - 5y^2 = 1$, and the odd pairs $\{\pm x_{2n+1}, \pm y_{2n+1}\}$ are solutions of $x^2 - 5y^2 = -1$. The method of descent can now be used to show that this list of solutions is complete. Indeed, this idea can be used for any d to show that if Pell's equation has one non-trivial solution, then it has infinitely many. See the exercises.

3.4.1. Theorem. *All solutions of the equation $x^2 - 5y^2 = \pm 1$ are given by the pairs $\{\pm x_n, \pm y_n\}$ for $n \geq 0$ obtained from the identities*

$$x_n + y_n\sqrt{5} = (2 + \sqrt{5})^n.$$

This leads to the recursive formulae

$$x_0 = 1,\ y_0 = 0 \quad \textit{and} \quad x_{n+1} = 2x_n + 5y_n,\ y_{n+1} = x_n + 2y_n \quad \textit{for } n \geq 0.$$

Proof. First note that from the previous discussion, the pairs $\{\pm x_n, \pm y_n\}$ for $n \geq 0$ are indeed solutions. From this formula, we obtain

$$\begin{aligned} x_{n+1} + y_{n+1}\sqrt{5} &= (x_n + y_n\sqrt{5})(2 + \sqrt{5}) \\ &= (2x_n + 5y_n) + (x_n + 2y_n)\sqrt{5}. \end{aligned}$$

So the recursive equations for x_{n+1} and y_{n+1} follow immediately.

Suppose that the set S of non-negative integer solutions which are not in this list is non-empty. We can then choose the solution $\{x, y\}$ so that y is as small as possible. The plan is to use Fermat's method of infinite decent to show that there is a smaller solution in S, a contradiction and hence $S = \varnothing$ and our list must be complete. The idea is that $x + y\sqrt{5}$ is a unit in $\mathbb{Z}[\sqrt{5}]$, as is $(2 + \sqrt{5})^{-1} = \sqrt{5} - 2$. Hence,

$$(x + y\sqrt{5})(\sqrt{5} - 2) = (5y - 2x) + (x - 2y)\sqrt{5}$$

is a unit. Thus, $\{5y - 2x, x - 2y\}$ is a solution.

The rest of the proof is just a computation to show that this is indeed a smaller positive solution that is not in our list. Since

$$4y^2 \leq 5y^2 \pm 1 = x^2 \leq 6y^2,$$

it follows that $2y \leq x < \sqrt{6}y$. Hence,

$$0 < (5 - 2\sqrt{6})y < 5y - 2x \leq 5y - 4y = y,$$

and

$$0 = 2y - 2y \leq x - 2y < (\sqrt{6} - 2)y < y.$$

Consequently, we have obtained a smaller non-negative solution than we started with. This solution cannot be $\{x_n, y_n\}$ from our list. For then,

$$\begin{aligned} x + y\sqrt{5} &= ((5y - 2x) + (x - 2y)\sqrt{5})(2 + \sqrt{5}) \\ &= (x_n + y_n\sqrt{5})(2 + \sqrt{5}) \\ &= x_{n+1} + y_{n+1}\sqrt{5}. \end{aligned}$$

Hence $(5y-2x, x-2y) \in S$, and $0 < x-2y < y$, contradicting the fact that (x, y) had the smallest 2nd coordinate in S. Therefore we have obtained the desired contradiction. ■

Exercises

1. Find all solutions of $x^2 - 2y^2 = \pm 1$.

2. Show by induction that the positive solutions of $x^2 - 5y^2 = \pm 1$ obtained above are given by the formulae

$$x_n = \frac{(2+\sqrt{5})^n + (2-\sqrt{5})^n}{2} \quad \text{and} \quad y_n = \frac{(2+\sqrt{5})^n - (2-\sqrt{5})^n}{2\sqrt{5}}.$$

The notation $\lceil x \rceil$ and $\lfloor x \rfloor$ mean the least integer $n \geq x$ and the least integer $m \leq x$ respectively. Deduce that

$$x_n = \lceil (2+\sqrt{5})^n/2 \rceil \quad \text{and} \quad y_n = \lfloor (2+\sqrt{5})^n/2\sqrt{5} \rfloor.$$

3. (a) Show that the elements of $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ are all elements of the form $\frac{a+b\sqrt{5}}{2}$ where $a \equiv b \pmod 2$.

(b) Show that the set of units of $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ have the form $\frac{\pm u_n \pm v_n\sqrt{5}}{2}$ where $\frac{u_n+v_n\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^n$ for $n \geq 0$.

(c) By Theorem 3.4.1, $2+\sqrt{5}$ is a unit. Where does it fit into this list?

4. Show that there are infinitely many Pythagorean triples with $y = x+1$; i.e., solutions of the form $(x, x+1, z)$.
HINT: reduce it to Pell's equation for $d = 2$. Hence find the smallest solution larger than $696^2 + 697^2 = 985^2$; i.e. $z > 985$?

5. Prove that if $x^2 - dy^2 = 1$ has one positive solution, then it has infinitely many. If $x^2 - dy^2 = -1$ has one positive solution, then it and $x^2 - dy^2 = 1$ have infinitely many solutions.

6. Show that $n^2 - 5m^2 = 11$ has infinitely many solutions.
HINT: this is the norm of an element in $\mathbb{Z}[\sqrt{5}]$.

7. Show that there are infinitely many positive integers a such that both $a+1$ and $3a+1$ are perfect squares.
HINT: reduce this to a question of elements in $\mathbb{Z}[\sqrt{3}]$ with specified norm.

3.5. The Gaussian Integers

When $d < 0$, the ring $\mathbb{Z}[\sqrt{d}]$ lies in the complex numbers $\mathbb{C}$, not the reals. For this section, some familiarity with complex numbers will be assumed. The ideas of complex numbers will be formally introduced in Chapter 5. We

use the notation $i = \sqrt{-1}$ for one (fixed) square root of -1. The **Gaussian integers** $\mathbb{Z}[\sqrt{-1}]$ consist of all complex numbers of the form $n + mi$ for integers n and m. The norm function is $N(n + mi) = n^2 + m^2$, and this is always a positive integer.

Let us find all of the units. For if $u = n+mi$ is a unit, then $n^2+m^2 = 1$. Hence one of n or m is 0 and the other is ± 1. So the units are ± 1 and $\pm i$.

We wish to establish unique factorization in this domain. By Theorem 1.8.18 and Remark 1.8.9, it is enough to show that the Gaussian integers are a Euclidean domain for the norm function, i.e. they have a division algorithm.

3.5.1. Proposition. *Suppose that $a, b \in \mathbb{Z}[\sqrt{-1}]$, and $a \neq 0$. Then there are elements $q, r \in \mathbb{Z}[\sqrt{-1}]$ such that $b = aq + r$ and $0 \leq N(r) < N(a)$.*

Proof. Since $b/a \in \mathbb{Q}[\sqrt{-1}]$, it can be written as $b/a = u+iv$ where u and v are rational. Pick integers n and m so that $|u-n| \leq 1/2$ and $|v-m| \leq 1/2$. Set $q = n + im$, and

$$r = b - aq = a(u + iv) - a(n + im) = a\big((u - n) + i(v - m)\big).$$

Then using the fact that $N(x)$ is defined on $\mathbb{Q}[\sqrt{-1}]$,

$$N(r) = N(a)\big(|u - n|^2 + |v - m|^2\big) \leq \frac{N(a)}{2}.$$

Thus the remainder r is sufficiently small. ■

3.5.2. Theorem. ***Unique Factorization for Gaussian Integers.*** *Suppose that a is a non-zero element of $\mathbb{Z}[\sqrt{-1}]$, and that it factors in two ways:*

$$a = up_1 \dots p_k = vq_1 \dots q_l,$$

where u and v are units and p_i and q_j are all primes. Then $k = l$ and there is a permutation π so that p_i and $q_{\pi(i)}$ are associates for $1 \leq i \leq k$.

Proof. By Proposition 3.5.1 and Remark 1.8.9, the hypotheses of Theorem 1.8.18 hold. So, the Gaussian integers have unique factorization. ■

In this ring, it is possible to describe all the primes. The argument will be split into two parts. The first theorem is of independent interest. The reader should notice that if item (5) were omitted from the list of equivalences, it would not appear to have anything to do with the Gaussian integers. However, the Unique Factorization theorem for this ring is crucial to the proof.

3.5.3. Theorem. *Let p be an odd prime. Then the following are equivalent:*

(1) $p \equiv 1 \pmod 4$.
(2) $x^2 + 1 \equiv 0 \pmod p$ *has a solution.*
(3) *There are integers n and m which are not multiples of p so that $p|n^2 + m^2$.*
(4) *p is the sum of two squares: $p = a^2 + b^2$.*
(5) *p factors as $p = (a + ib)(a - ib)$ in $\mathbb{Z}[\sqrt{-1}]$.*

Proof. Suppose that (1) holds, and write $p = 4n + 1$. Let $a = (2n)!$. Then by Wilson's Theorem,

$$\begin{aligned} a^2 &\equiv \Big(\prod_{j=1}^{2n} j\Big)\Big(\prod_{j=1}^{2n}(-j)\Big)(-1)^{2n} \\ &\equiv \prod_{j=1}^{2n} j(4n+1-j) \\ &\equiv (4n)! \equiv -1 \pmod p \end{aligned}$$

So a is a solution of (2).

If n is a solution of $x^2 + 1 \equiv 0 \pmod p$ and $m = 1$, then $n^2 + m^2$ is a multiple of p, so (3) holds.

Suppose that (3) holds. Notice that in $\mathbb{Z}[\sqrt{-1}]$, it is possible to factor $n^2 + m^2$ as $(n + im)(n - im)$. If p were prime in $\mathbb{Z}[\sqrt{-1}]$, it would divide one of $n \pm im$. This then implies that p divides both n and m, contrary to fact. Hence p has a proper divisor $x \in \mathbb{Z}[\sqrt{-1}]$. It follows that $N(x)$ is a proper divisor of $N(p) = p^2$. That is, $N(x) = p$. If $x = a + ib$, then $p = a^2 + b^2$. This proves (4) and (5). Since $a^2 + b^2 = (a + ib)(a - ib)$, we see (5) implies (4).

Finally, since p is odd, one of a, b is even and the other is odd. Therefore $p = a^2 + b^2 \equiv 1 \pmod 4$. So (4) implies (1). ■

3.5.4. Theorem. *The primes in $\mathbb{Z}[\sqrt{-1}]$ are:*

(1) *The elements of prime order: the primes $\pm 1 \pm i$ of norm 2; and the elements x with $N(x) = p$, where p is a prime congruent to 1 (mod 4).*
(2) *The elements $\pm p$ and $\pm ip$ where p is a prime integer with $p \equiv 3 \pmod 4$.*

Proof. By Lemma 3.3.6, it follows that if $N(x)$ is prime, then x is prime. For $N(x)$ to be prime, x cannot be an integer or i times an integer (these elements have square norms). So $x = a + ib$, and a and b are not both even (because 2 does not divide x.) Hence $p = N(x) = a^2 + b^2$ is the sum of squares, not both even. Thus, it must be congruent to 1 or 2 modulo 4.

Now 2 is the only prime congruent to 2 (mod 4), and one checks that $\pm 1 \pm i$ are the only elements of norm 2. The others have odd prime norm. Suppose that p is an integer prime congruent to 3 mod 4. If this were not prime in $\mathbb{Z}[\sqrt{-1}]$, it would factor as $p = xy$, say. But then

$$p^2 = N(p) = N(x)N(y).$$

Neither $N(x)$ nor $N(y)$ is 1, so $N(x) = N(y) = p$. But $p \equiv 3 \pmod 4$, and this is impossible for a norm which is a sum of two squares. Hence p is prime in $\mathbb{Z}[\sqrt{-1}]$. Its associates $\pm p$ and $\pm ip$ are then also prime.

It remains to show that there are no other primes. Let $x = n + mi$ be a prime in $\mathbb{Z}[\sqrt{-1}]$. Its conjugate $\tilde{x} = n - mi$ is also a prime. To see this, notice that $x = ab$ if and only if $\tilde{x} = \tilde{a}\tilde{b}$. So any factorization of $\tilde{x}$ into proper factors implies that x also factors, contrary to fact.

Consider $N(x) = x\tilde{x}$. If this is prime, it falls into case (i). Otherwise, $N(x)$ factors non-trivially in the integers as

$$x\tilde{x} = N(x) = pq.$$

Now we can apply the Unique Factorization Theorem. The left-hand side is the product of two primes. So the right-hand side must also be a factorization into primes. Furthermore, x is the associate of one, say p, and $\tilde{x}$ is the associate of the other, q. But if u is a unit so that $x = up$, then $\tilde{x} = \tilde{u}\tilde{p} = \tilde{u}p$. Hence p is an associate of $\tilde{x}$, and hence also an associate of q. This means that $p = q$ is a prime.

There are two cases. If $x = \pm p$ or $\pm ip$, this falls into case (ii). Otherwise, $x = n + im$, where n and m are not multiples of p, but $n^2 + m^2 = p^2$ is divisible be p. So by Theorem 3.5.3, $p \equiv 1 \pmod 4$. But then, by the same theorem, we find out that p (and so also x) is not prime in $\mathbb{Z}[\sqrt{-1}]$. That eliminates this final possibility. ■

A pretty application of this is a complete description of which numbers can be expressed as the sum of two squares. The key additional piece of information needed is the following computation. The proof is left to the reader.

3.5.5. Lemma. *Let a, b, x, and y be integers. Then*

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2.$$

3.5.6. Theorem. *Let n be a positive integer. Factor n as $n = ab^2$ where a is square free. Then n can be expressed as the sum of two squares if and only if a has no prime factors congruent to* 3 (mod 4).

Proof. First suppose that a has no prime factors congruent to 3 (mod 4). By Theorem 3.5.3, each factor of a is the sum of two squares. Repeated application of the lemma shows that their product is also the sum of two squares. Finally, multiplying by b^2 preserves this as the sum of two squares.

Conversely, suppose that $n = x^2 + y^2$, and that p is a factor of a. Let k be the largest power of p which divides both x and y. Set $X = x/p^k$, $Y = y/p^k$, and $N = n/p^{2k}$. Then since an *odd* power of p divides n, N is still a multiple of p but X and Y are not. By Theorem 3.5.3, $p = 2$ or $p \equiv 1 \pmod 4$. ■

3.5.7. Example. As a second application, let us consider a Diophantine equation:

$$x^2 + 4 = z^3.$$

It is convenient to work in $\mathbb{Z}[\sqrt{-1}]$ rather than in the integers because $x^2 + 4 = z^3$ factors to obtain

$$z^3 = (x + 2i)(x - 2i).$$

First suppose that each of $x \pm 2i$ are cubes, so that there are integers a and b with

$$x + 2i = (a + bi)^3 = (a^3 - 3ab^2) + i(3a^2b - b^3).$$

Hence,

$$(3a^2 - b^2)b = 2.$$

Since b divides 2, it must be ± 1 or ± 2. Checking each case provides the solution $a = \pm 1$, $b = 1$ or -2. Therefore $x = a^3 - 3ab^2 = \pm(1 - 3b^2) \in \{\pm 2, \pm 11\}$. This yields the two positive solutions

$$2^2 + 4 = 2^3 \quad \text{and} \quad 11^2 + 4 = 5^3.$$

Let us show that these are the only solutions. Suppose that (x, y, z) is a positive solution. Let p be a prime in $\mathbb{Z}[\sqrt{-1}]$ which divides z. If p^m is the greatest power of p which divides z, then p^{3m} divides z^3. If p divides only one of $x \pm 2i$, say $x + 2i$, then p^{3m}, which is a perfect cube, divides $x + 2i$. However, p might divide both $x \pm 2i$. In that case, it divides

$$\gcd(x + 2i, x - 2i) = \gcd(x + 2i, 4).$$

Since $4 = -(1+i)^4$, this means $p = 1+i$. Now p is associated to $-i(1+i) = 1 - i = \tilde{p}$. Thus if p^k divides $x + 2i$, then $\tilde{p}^k$ divides $(x + 2i)\tilde{} = x - 2i$. That is, the multiplicity of p as a factor of $x + 2i$ and $x - 2i$ are equal. Thus, $3m$ is even, say $3m = 6n$. Hence, $x \pm 2i$ are both multiples of p^{3n} which is also a perfect cube. It follows that except for the factor of a unit, both $x \pm 2i$ are perfect cubes. But the units, $\pm i$ and ± 1, are all perfect cubes. So, $x \pm 2i$ are both cubes. Therefore we have found all the solutions.

Exercises

1. Factor 1105 completely in $\mathbb{Z}[\sqrt{-1}]$.

2. Solve the Diophantine equation $x^2 + 44^2 = z^6$.

3. Show that $\mathbb{Z}[\sqrt{-2}]$ has a division algorithm. Hence deduce that $\mathbb{Z}[\sqrt{-2}]$ has unique factorization.

4. Find all solutions of $x^2 + 2 = y^3$.

5. Give another argument to find all irreducible Pythagorean triples (x, y, z), i.e. $x^2 + y^2 = z^2$ and $\gcd(x, y) = 1$, as follows.
(a) Assume that x is odd. Factor $x^2 + y^2 = (x + iy)(x - iy) = z^2$ in $\mathbb{Z}[\sqrt{-1}]$. Prove that $x + iy$ is a square.
(b) Hence find a formula for x, y and z.
(c) Verify that every triple of this form yields an irreducible Pythagorean triple.

6. (**Zagier**) Let p be a prime with $p \equiv 1 \pmod 4$. Define

$$S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}.$$

Also define $T : S \to S$ by

$$T(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) & \text{if} \quad x < y - z \\ (2y - x, y, x - y + z) & \text{if} \quad y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if} \quad x > 2y. \end{cases}$$

(a) Prove that S is finite, $T(S) \subset S$ and $T \circ T = id$.
(b) Prove that T has a unique fixed point $(x_0, y_0, z_0) = T(x_0, y_0, z_0)$. Deduce that $|S|$ is odd.
HINT: Note that a fixed point has the form (x, x, z), which forces $x|p$.
(c) Let $J(x, y, z) = (x, z, y)$. Show that $J(S) = S$. Using that $|S|$ is odd, prove that J has a fixed point.
(d) Deduce that p is a sum of two squares.

7.★ Find all solutions of $x^2 + 11 = y^3$. You must work in $\mathbb{Z}[\sqrt{-11}]$, which is a Euclidean domain.

3.6. Quadratic Reciprocity

Primitive roots can be used to analyze simple congruence equations. Recall that a is a primitive root modulo a prime p if $\{a^k : 1 \le k \le p-1\}$ represent all $p - 1$ distinct non-zero equivalence classes $\pmod p$. Thus every $x \in \mathbb{Z}_p^*$ has the form $x = a^k$ for some k. We can use this to solve certain congruence equations.

3.6.1. Example. Consider the equation

$$(\ddagger) \qquad x^6 \equiv 13 \pmod{17}.$$

Of course, trial and error works for such a small number. However, let us instead make use of the fact that 3 is a primitive root of $\mathbb{Z}_{17}$ (because

$3^8 \equiv -1 \pmod{17}$). A calculation shows that $3^4 \equiv 13 \pmod{17}$. Equation (‡) has a solution $x = 3^k$ if and only if

$$x^6 \equiv 3^{6k} \equiv 3^4 \pmod{17}.$$

Hence $3^{6k-4} \equiv 1 \pmod{17}$. This occurs exactly when $6k \equiv 4 \pmod{16}$. Since $\gcd(6, 16) = 2$ divides 4, equation (‡) has the solutions $k \equiv 6 \pmod 8$ or $k \equiv 6, 14 \pmod{16}$. Thus the solutions are $x \equiv 3^6 \equiv 15 \pmod{17}$ and $x \equiv 3^6 3^8 \equiv 2 \pmod{17}$.

On the other hand, consider the equation

$$x^6 \equiv 3 \pmod{17}.$$

Again if we set $x = 3^k$, the equation becomes

$$x^6 \equiv 3^{6k} \equiv 3^1 \pmod{17}.$$

This has solutions $x = 3^k$ satisfying $6k \equiv 1 \pmod{16}$. This has no solutions because $\gcd(6, 16) = 2$ does not divide 1.

The general result along these lines is proved in the same way. The added twist is that we obtain a condition that does not use primitive roots! However, the *existence* of primitive roots is used in the proof.

3.6.2. Theorem. *Let p be a prime, let n be a positive integer, and suppose that $gcd(b, p) = 1$. Set $s = \gcd(n, p-1)$ and $t = (p-1)/s$. Then the congruence equation $x^n \equiv b$ has solutions if and only if $b^t \equiv 1 \pmod p$. In this case, there are s distinct solutions modulo p.*

Proof. Let a be a primitive root mod p. Let m be chosen so that $b \equiv a^m \pmod p$. Then $x^n \equiv b \pmod p$ has a solution $x \equiv a^k$ if and only if $x^n \equiv a^{nk} \equiv a^m$, which happens if and only if $nk \equiv m \pmod{p-1}$. By Theorem 2.6.1, this has solutions exactly when $s = gcd(n, p-1)$ divides m. But $s|m$ if and only if $p-1|tm$. Since a is a primitive root, $a^e \equiv 1 \pmod p$ exactly when e is a multiple of $p-1$. Thus our equation has a solution if and only if

$$1 \equiv a^{tm} \equiv \left(a^m\right)^t \equiv b^t \pmod p.$$

Moreover, the solution of $nk \equiv m \pmod{p-1}$ is unique modulo t; so that there are exactly s solutions modulo $p-1$. Thus, when solutions exist, there are exactly s distinct solutions. ■

We apply this result for $n = 2$ and $p > 2$. Note that $s = \gcd(2, p-1) = 2$; whence $t = \frac{p-1}{2}$.

3.6.3. Corollary. *An number b is a square modulo an odd prime p if and only if*

$$b^{(p-1)/2} \equiv 1 \pmod p.$$

3.6.4. Corollary. *$x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

Proof. For $p = 2$, $1^2 = 1 \equiv -1 \pmod{2}$. For $p > 2$, write $p = 4n + e$ where $e \in \{1, 3\}$. The previous corollary shows that -1 is a square modulo p if and only if $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. However

$$(-1)^{(p-1)/2} \equiv (-1)^{(e-1)/2} \equiv \begin{cases} 1 \pmod{p} & \text{if } e = 1 \\ -1 \pmod{p} & \text{if } e = 3 \end{cases}$$

That is, -1 is a square if and only if $p = 2$ or $p \equiv 1 \pmod{4}$. ■

Gauss was interested in the problem of deciding when a number b was congruent to a square modulo a prime p. He gave an elegant solution which allows the calculations to be carried out easily by hand. The key result became known as the Law of Quadratic Reciprocity. This was one of Gauss's most celebrated theorems.

3.6.5. Definition. The **quadratic residue** of a modulo a prime p is 1 if a is a square modulo p, and -1 if it is not. It is denoted by $\left(\frac{a}{p}\right)$.

The corollary above shows that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Hence it follows that

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

In other words, the quadratic residue is multiplicative. So in order to do computations, it suffices to know $\left(\frac{q}{p}\right)$ when p and q are primes. This is the content of Gauss's famous theorem, which we prove below.

3.6.6 Law of Quadratic Reciprocity. *Suppose that p and q are odd primes. Then*

(1) $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

(2) $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

The quantity $\frac{p^2-1}{8}$ appears here. If $p = 8a \pm 1$, then $\frac{p^2-1}{8} = \frac{64a^2 \pm 16a}{8}$ is even; and if $p = 8a \pm 3$, then $\frac{p^2-1}{8} = \frac{64a^2 \pm 48a + 8}{8}$ is odd.

The following computational lemma will calculate $\left(\frac{a}{p}\right)$ in a different way. The proof is tricky.

3.6.7. Lemma. *Let p be an odd prime and a be relatively prime to p. Let $0 < r_i < p$ be such that $ai \equiv r_i \pmod p$ for $1 \le i \le \frac{p-1}{2}$. Let*

$$n = \left|\left\{i : 1 \le i \le \frac{p-1}{2} \text{ and } r_i > \frac{p}{2}\right\}\right| \quad \text{and} \quad N = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor.$$

Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Furthermore, $N \equiv n + (a-1)\frac{p^2-1}{8} \pmod 2$. In particular, if a is odd, then

$$\left(\frac{a}{p}\right) = (-1)^N.$$

Proof. Let $b_1, \dots, b_m$ be the $r_i < \frac{p}{2}$, and let $c_1, \dots, c_n$ be the $r_i > \frac{p}{2}$. Then $m + n = \frac{p-1}{2}$. Observe that if $1 \le i < j \le \frac{p-1}{2}$,

$$r_i \pm r_j \equiv a(i \pm j) \equiv 0 \pmod p \iff i \pm j \equiv 0 \pmod p \implies i = j.$$

Therefore $b_1, \dots, b_m, p - c_1, \dots, p - c_n$ are distinct. Since $m + n = \frac{p-1}{2}$ and the b_i and $p - c_j$ all lie between 1 and $\frac{p-1}{2}$, we see that

$$\{b_1, \dots, b_m, p - c_1, \dots, p - c_n\} = \{1, \dots, \tfrac{p-1}{2}\}.$$

Thus,

$$\begin{aligned}(\tfrac{p-1}{2})! &= \prod_{i=1}^{m} b_i \cdot \prod_{j=1}^{n} (p - c_j) \equiv (-1)^n \prod_{i=1}^{m} b_i \cdot \prod_{j=1}^{n} c_j \\ &\equiv (-1)^n \prod_{i=1}^{(p-1)/2} (ia) = (-1)^n a^{(p-1)/2} (\tfrac{p-1}{2})! \pmod p.\end{aligned}$$

and hence

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod p.$$

We now turn to the computation of N. First observe that $ia = p\lfloor \frac{ia}{p} \rfloor + r_i$. Thus, we have

$$\begin{aligned}\sum_{i=1}^{(p-1)/2} r_i &= \sum_{i=1}^{(p-1)/2} \left(ia - p\left\lfloor \frac{ia}{p} \right\rfloor\right) \\ &= a\frac{1}{2}\frac{p-1}{2}\left(\frac{p-1}{2} + 1\right) - Np = a\frac{p^2-1}{8} - Np.\end{aligned}$$

On the other hand, working mod 2, we have

$$\sum_{i=1}^{(p-1)/2} r_i \equiv \sum_{i=1}^{m} b_i + \sum_{j=1}^{n} \big((p - c_j) - p\big)$$
$$= -np + \sum_{i=1}^{(p-1)/2} i = -np + \frac{p^2-1}{8} \pmod 2.$$

Therefore, the two quantities just computed are equal modulo 2; whence

$$N - n \equiv (N-n)p \equiv (a-1)\frac{p^2-1}{8} \pmod 2.$$

When a is odd, $N \equiv n \pmod 2$; and so $\left(\frac{a}{p}\right) = (-1)^N$. ■

3.6.8. Theorem. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Proof. By Lemma 3.6.7, we must count the number of elements n in the set $\{2, 4, 6, \ldots, p-1\}$ which are greater than $\frac{p}{2}$. If $p \equiv 3 \pmod 4$, then smallest such even integer is $\frac{p+1}{2}$; and if $p \equiv 1 \pmod 4$, then smallest such element is $\frac{p+3}{2}$.

We first consider the case $p \equiv 1 \pmod 4$. Then

$$n = 1 + \frac{p - 1 - \frac{p+3}{2}}{2} = \frac{p-1}{4} \equiv \begin{cases} 0 \pmod 2 & \text{if } p \equiv 1 \pmod 8 \\ 1 \pmod 2 & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Similarly, when $p \equiv 3 \pmod 4$,

$$n = 1 + \frac{p - 1 - \frac{p+1}{2}}{2} = \frac{p+1}{4} \equiv \begin{cases} 1 \pmod 2 & \text{if } p \equiv 3 \pmod 8 \\ 0 \pmod 2 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Therefore $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \pmod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 \pmod 8$. Thus, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. ■

We are now ready to prove the Law of Quadratic Reciprocity.

Proof of Theorem 3.6.6. The first statement was established above in Theorem 3.6.8. For the second statement, let

$$N = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \quad \text{and} \quad M = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor.$$

Since p and q are odd, Lemma 3.6.7 shows that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N}.$$

Consider the rectangle

$$R = \{(x, y) \in \mathbb{Z}^2 : 1 \leq x \leq \frac{p}{2},\ 1 \leq y \leq \frac{q}{2}\}.$$

Notice that

$$|R| = \left\lfloor \frac{p}{2} \right\rfloor \left\lfloor \frac{q}{2} \right\rfloor = \frac{p-1}{2}\,\frac{q-1}{2} = \frac{(p-1)(q-1)}{4}.$$

By counting $|R|$ in a different way, we will see it is also equal to the quantity $M + N$. Consider the line $L \subset \mathbb{R}^2$ defined by the equation $y = \frac{q}{p}x$. Since p and q are distinct primes, we see that $L \cap R = \emptyset$. Divide R into two triangles

$$T_1 = \{(x, y) \in R : y < \frac{q}{p}x\} \quad \text{and} \quad T_2 = \{(x, y) \in R : x < \frac{p}{q}y\}.$$

Then $|R| = |T_1| + |T_2|$. For each $1 \leq i \leq \frac{p-1}{2}$,

$$\left|\left\{(i, y) : 1 \leq y \leq \frac{q}{2}\right\} \cap T_1\right| = \left|\left\{y \in \mathbb{Z} : 1 \leq y < \frac{iq}{p}\right\}\right| = \left\lfloor \frac{iq}{p} \right\rfloor.$$

Hence

$$|T_1| = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor = N.$$

Similarly, for each $1 \leq j \leq \frac{q-1}{2}$,

$$\left|\left\{(x, j) : 1 \leq x \leq \frac{p}{2}\right\} \cap T_2\right| = \left|\left\{x \in \mathbb{Z} : 1 \leq x < \frac{ip}{q}\right\}\right| = \left\lfloor \frac{ip}{q} \right\rfloor.$$

Thus, $|T_2| = M$. Therefore $N + M = |R| = \frac{(p-1)(q-1)}{4}$, and so

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

This finishes the proof. ■

Exercises

1. Determine if 107 is a quadratic residue modulo 1009.

2. Determine if 20964 is a quadratic residue modulo 1987.

3. Find all solutions to the equation $x^5 \equiv 29 \pmod{61}$.

4. Without using Theorem 3.6.6, show that for every prime p, at least one of -1, 2 and -2 is a square modulo p.

5. Let p be a prime and let $a, b \in \mathbb{N}$ with p not dividing a or b. Show that exactly 1 or 3 of a, b, ab are squares modulo p.

6. For prime $p \geq 7$, show that there are always two consecutive quadratic residues mod p neither of which is zero.

7. Let p be a prime in $\mathbb{Z}$ and suppose 5 is not prime in $\mathbb{Z}[\sqrt{p}]$. Prove that $p = 5$ or $p \equiv \pm 1 \pmod 5$.

8. (a) If p is an odd prime, show that $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$.

(b) Find a similar formula for $\left(\frac{5}{p}\right)$.

9. (a) Let p be an odd prime. Consider the equation

$$ax^2 + bx + c \equiv 0 \pmod p$$

where p does not divide a. Let $d = b^2 - 4ac$ and $y = 2ax + b$. Reduce this equation to $y^2 \equiv d \pmod p$ and hence obtain a quadratic formula modulo p.

(b) Find a necessary and sufficient condition for this quadratic to have a root when $p = 2$.

Notes on Chapter 3

Diophantine equations are named after the Greek mathematician Diophantus of the 3rd century CE. Linear Diophantine equations were discussed in the notes in Chapter 2.

Much earlier, in the 6th century BCE, Pythagorus gave examples of integral Pythagorean triples and produced an infinite family. Later Plato found another non-trivial infinite family. Independently the Hindu scholars also found similar families. Around 300 BCE, Euclid gave more general families of solutions in his *Elements*. Many schools of mathematics around the world eventually solved this problem.

Fermat studied ways of representing numbers as sums of squares, cubes, etc. He showed that a prime $p \equiv 1 \pmod 4$ is a sum of two squares in a unique way. He also knew that if n has a prime factor $p \equiv 3 \pmod 4$ to an odd power, then it is not a sum of two squares. The final form was due to Euler.

Fermat wrote about his equation $x^n + y^n = z^n$ in his notes. However in communications with others, he did not claim a solution. He did show the impossibility of $x^4 + y^4 = z^2$. He may also have had a solution for $n = 3$, since he challenged other mathematicians to solve it, although there is no record of his solution. Euler solved $n = 3$. Legendre and Dirichlet solved $n = 5$. The case $n = 7$ was due to Lamé, and was simplified by Lebesgue. The first significant general theorem was due to Sophie Germain. Kummer developed ideas of modern ring theory in order to analyze the failure of unique factorization in various number domains. He used this to provide a

proof for all *regular primes*. The smallest cases remaining open after that were 37 and 59.

Mordell made a conjecture in the 1920's which, if true, would imply that equations like Fermat's for $n \geq 3$ could have at most finitely many solutions. This was proved by Faltings in 1983, and he received the Fields medal for this work. By 1993, computers had been used to show that Fermat's equation had no solutions for $n \leq 4\,000\,000$. In 1955, Shimura and Taniyama proposed a conjecture concerning elliptic curves and modular forms. It was later shown by work of Ribet that this conjecture implies the truth of Fermat's claim. In 1993, Wiles announced a solution to a major case of this conjecture which implied Fermat's last theorem. It turned out that there was a non-trivial gap which was later fixed by Wiles and Taylor. Breuil, Conrad, Diamond and Taylor proved the full Shimura–Taniyama Conjecture in 2001.

Pell's equation also has a long history back to antiquity. Bhaskara gave a general method for solution in 1150. He explicitly solved $x^2 - 61y^2 = 1$, giving the smallest solution $x = 1\,766\,319\,049$ and $y = 226\,153\,980$. Lagrange proved that Bhaskara's method worked in 1738. He later developed a complete solution using continued fractions. Fermat found a solution for $d \leq 150$ and challenged British mathematicians to solve the cases $d = 151$ or $d = 313$. This was done by Broukner. However Euler mistakenly attributed this to Pell, and his name has stuck in spite of it being incorrect.

The quadratic reciprocity laws were conjectured by Euler and Legendre. Legendre made substantial progress on the problem and introduced the Legendre symbol $\left(\frac{p}{q}\right)$. Gauss published a complete solution in his treatise *Disquisitiones Arithmeticae* in 1798.

See [**9**, Vol.II] for an extensive history of these problems, or consult the books by Cooke [**8**] and Kleiner [**20**]. See the article [**22**] for more information about the work of Sophie Germain. See Ribenboim's book *Fermat's last theorem for amateurs* [**30**] for more information on Fermat's last theorem. See Stark [**37**] for the solution to Pell's equation using continued fractions. Hardy and Wright [**15**] also contains much historic information, as well as the mathematics including a proof of the law of quadratic reciprocity.

Chapter 4

Codes and Factoring

In this chapter, we will look at a code based on the number theoretic properties that we have developed. Since this code depends on the fact that it is a lot easier to find big primes than to factor large numbers, we will also study how this is done.

4.1. Codes

Codes are a way of **encrypting** a message so that it is very difficult or impossible to read the message unless you have knowledge of the **key** which *unlocks* the message. The most familiar codes are simple substitution codes. This means that each letter is replaced with another one. For example, consider the permutation of the alphabet given by

```
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ
5936071842KSRIUFHQPOWELJGYTADZMVXNBC
```

A message like 'Houston airport, noon, Jan 22' would become

'QGMDZGJKPAYGAZJGGJOKJ33'.

This kind of code is very easy to break with the aid of a computer. In fact, with a longer message, it can be done by hand and is a popular pastime for many people. For example, this message has 5 G's, so one might think this is a vowel.

Actually, computers routinely use codes all the time—not for secrecy, but because computers can only store numbers (base 2). The ASCII code provides a number from 0 to 255 for all digits, upper and lower case letters, and many other symbols. This is how the computer can store text, and how word processors can manipulate it. The modern UTF-8 system extends ASCII and encodes over 1,000,000 characters containing all major alphabets in the world. A character uses up to 4 bytes (32 bits), so there are 2^{32} possibilities. Since there is extra room in this system, certain bits are used to detect and possibly correct errors. This is another important use of encryption that helps ensure accurate transmission of digital data.

It is much more difficult to break the code known as a 'one time pad'. The idea is to code your message by using another message known to the encoder and the intended recipient. First we need a simple way to combine two letters into one. Let us use a 36 letter alphabet consisting of 26 letters and 10 decimal digits. We can think of each letter as representing an element in $\mathbb{Z}_{36}$. That is.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Then two letters can be combined by addition modulo 36. Let us use the message 'The quick brown fox jumped over the lazy dog' to encode our message 'Pizza 5:30 tonight'. Consider

P	I	Z	Z	A	5	3	0	T	O	N	I	G	H	T
T	H	E	Q	U	I	C	K	B	R	O	W	N	F	O
I	Z	D	P	4	N	F	K	4	F	B	E	3	6	H

To decode this, one needs to know the coding message. If this message is changed every time, for example using different pages of *War and Peace* each time, this is virtually impossible to break without stealing the code. However, if both the sender and the recipient always have their copy of *War and Peace* with them, it might be a giveaway.

One thing these two codes have in common with each other and most other codes is that encoding and decoding use the same information. Another kind of code has been invented which is of quite a different character. Known as public key cryptography, the interesting thing about these codes is that the method for encryption can be made public. For example, the code can be published in the *New York Times* or be listed on an electronic bulletin board. Anyone can send you a coded message. The important point is that knowing how to *encode* does not tell you how to *decode*!

4.2. The Rivest-Shamir-Adelman Scheme

The public key code that we will study was developed at MIT by Rivest, Shamir and Adelman. The key point that makes their code secure is that it is very easy to find large primes (say 200–300 decimal digits), but very difficult to factor large numbers that have a small number of large prime factors. The reason for this will be discussed in the next section.

Here is how it works. Pick two large primes p and q, with 200–300 digits. Set $n = pq$, and notice that $\varphi(n) = (p-1)(q-1)$. Now pick another number r (say 6–10 digits) which is relatively prime to $\varphi(n)$. Publish the two numbers (n, r).

Anyone who wishes to send you a message does the following. First turn your message into a number M by some standard scheme such as ASCII

or any simple scheme that encodes the 36 characters 0–9 and A–Z as a two digit number, possibly also including a–z and some punctuation marks. If necessary, split your message into blocks so the numbers encoded are all less than n. The coded message is

$$C \equiv M^r \pmod{n}.$$

This message can now be published in the personals section of the *New York Times*, or posted somewhere online.

The presumption is that all interested parties know the method of encoding and the message sent. Nevertheless, it is secure! Only you can break the code. To do this, you must know p and q. And you must know the Chinese Remainder Theorem. First, solve the equation

$$rs \equiv 1 \pmod{\varphi(n)}.$$

This has a unique solution by Lemma 2.3.3. Of course, to find s it is necessary to know $\varphi(n)$, and to find it, one must factor n. The key is Euler's Theorem, which tells us that $M^{\varphi(n)} \equiv 1 \pmod{n}$ when $\gcd(M, n) = 1$. In fact, since n is the product of two distinct primes, it turns out that our decoding method works for every M in the interval $0 < M < n$. Since $rs \equiv 1 \pmod{\varphi(n)}$, it can be written as $rs = 1 + k\varphi(n)$. Now compute $C^s \pmod{n}$ using the Chinese Remainder Theorem.

$$C^s \equiv M^{rs} \equiv M^1 (M^{p-1})^{k(q-1)} \equiv M \pmod{p}$$
$$C^s \equiv M^{rs} \equiv M^1 (M^{q-1})^{k(p-1)} \equiv M \pmod{q}$$

By the Chinese Remainder Theorem, $C^s \equiv M \pmod{n}$. Of course this only finds M up to a multiple of n. That is why we begin with a message such that $0 < M < n$.

If you have access to a symbolic manipulation software, try to design your own codes. Exchange messages with a friend, and decode them. Try using these same programs to break your friend's code.

The message is as secure as the difficulty of factoring large numbers (not practical) and the security of the storage location of the key s. (It is not necessary to remember p and q.) The latter consideration does not have anything to do with coding though. Of course, if everyone knows your encoding procedure, what prevents them from sending you a message and signing another name? How can you be sure that the message is really from your friend? The trick is for the sender to use his own code to give the message a **signature**.

It works like this: suppose your code is (n, r) and the sender has a published code (N, R). Let us also suppose that $N < n$. Only the sender knows the decoding key S for the (N, R) code. The sender computes

$$Q \equiv M^S \pmod{N} \quad \text{and} \quad 0 \leq Q < N.$$

Then this is encoded by the (n, r) code by

$$C \equiv Q^r \pmod{n}.$$

Again C is sent. To decode, you compute

$$Q \equiv C^s \pmod{n}.$$

Fortunately, since $N < n$, we know that $0 < Q < n$ without any ambiguity. Now using the sender's published code, compute

$$M \equiv Q^R \pmod{N}.$$

This message must be from our friend because only he/she knows S which enabled the encoding in the first place.

What happens if $N > n$? Try it out on a computer. You will end up with garbage. In this case you must encode using n first:

$$Q \equiv M^r \pmod{n}$$
$$C \equiv Q^S \pmod{N}.$$

This is decoded in the same basic way.

We end this section by discussing two practical aspects of the Rivest-Shamir-Adelman scheme. First, the encryption scheme involves raising M to a potentially large power r. If one computes M^r by naively multiplying M with itself r times, this requires r computations, which is a large number. Instead, the way one performs this computation in practice is expand r in base 2, namely write

$$r = a_0 + 2a_1 + 4a_2 + \ldots + 2^k a_k$$

where each $a_i \in \{0, 1\}$. Then, by repeatedly squaring, one computes M, M^2, $M^4 = (M^2)^2$, $M^8 = (M^4)^2$, ..., $M^{2^k} = (M^{2^{k-1}})^2$ mod n. One then computes the product

$$M^r \equiv M^{a_0}(M^2)^{a_1} \ldots (M^{2^k})^{a_k} \pmod{n}.$$

In total, this requires very few computations. To obtain all powers M^{2^r} for $r \leq s$ involves taking $k - 1$ products, and then obtaining M^r involves $a_0 + \cdots + a_k - 1 \leq k$ products. Thus, this is on the order of $2k \approx 2\log_2(r)$ computations, which is substantially faster than performing r computations.

Second, the Rivest-Shamir-Adelman scheme relies on choosing $n = pq$ with p and q large primes, which raises the question of how one obtains large primes in practice. At the beginning of Section 1.4, we mentioned the famous Prime Number Theorem, which asserts that for large N, there are roughly $\frac{N}{\log(N)}$ prime numbers less than or equal to N. Said differently, if we fix a large number N, the probability that a randomly chosen number $m \in \{1, \ldots, N\}$ is prime is roughly $\frac{1}{\log(N)}$. Therefore, if we choose $\log(N)$ numbers in $\{1, \ldots, N\}$, there is a good chance that at least one of them is prime. The chances are much higher if you avoid multiples of small primes. In practice, one can test primality using the deterministic algorithm by Agrawal-Kayal-Saxena developed in 2004 or the older Miller-Rabin probabilistic test. Notice that even if N is a large number with 500 digits, $\log(N)$

is only about 1000, so finding large primes with this method is quite practical for a computer.

Exercises

1. Show that s works as a key to decode the RSA encoded message provided that

$$rs \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}.$$

2. Use computer software to check that $r = 42385687$ and a number 2 lines long:

$n = 91875320684918502380129870007406274898925429401183797214111268335816454459464037326759995364752417$

has a decoder

$s = 56970378770327971563435212231376282085305478725834255953360930453245246857516891597701705638306003$

3. Use computer software to choose two primes p, q with 40–45 decimal digits, and construct an RSA code.

4. Exchange messages with a friend. Code your student id number or a simple message with your code 'signature', then code it up using your friend's code.

5. Try to break your friend's code.

4.3. Primality Testing

How do you tell if a large number is composite or prime without doing a lot of trial divisions? It turns out that you may be able to show that a number is composite without knowing any factors! In 2004, Agrawal-Kayal-Saxena gave a groundbreaking efficient algorithm to determine if a number is prime. Their algorithm uses the fact that if $n \geq 2$ and $\gcd(a, n) = 1$, then n is prime if and only if $(X + a)^n \equiv X^n + a^n \pmod{n}$, see Exercise 1. Checking this particular congruence is not efficient. However they modify it in a way that makes the problem tractable: if $(X + a)^n \equiv X^n + a^n \pmod{n}$ holds, then it is also true that for all r, there are polynomials $f(X), g(X)$ such that

$$(X + a)^n = (X^n + a^n) + (X^r - 1)g(x) + nf(X). \tag{4.3.1}$$

Indeed, we can simply take $g = 0$ and f an appropriate polynomial. Agrawal-Kayal-Saxena show a converse result: they prove that if there exists r and a set of a such that if (4.3.1) holds for some f and g, then n is a prime power. Moreover, they make these choices in such a way that this equation can be checked efficiently. Although the details of their algorithm are beyond the scope of this course, in this section we highlight some other methods to test primality.

One guaranteed way to test if a number p is prime is based on the results of Section 2.10. We showed in Theorem 2.10.6 that if p is prime, then there is a number a such that the set of powers $\{a, a^2, a^3, \ldots, a^{p-1}\}$ modulo p is a permutation of the list $\{1, 2, 3, \ldots, p-1\}$. Conversely, the existence of such an element guarantees that there are $p-1$ different numbers relatively prime to p. This means that p is prime. Indeed, there are $\varphi(p-1)$ such generators. So chances of finding one by trial and error are quite good. The problem, however, with this test is that if p is large, it is time-intensive to compute all powers of a number a. In this section, we discuss more efficient algorithms to test primality.

Like the Rivest-Shamir-Adelman code, the key to a more efficient algorithm comes from Fermat's Theorem. Let us suppose that a large number n is given. We know that if n is prime, then $a^{n-1} \equiv 1 \pmod{n}$. So if $a^{n-1} \not\equiv 1 \pmod{n}$ for some a, then n is definitely composite. For example, if $n = 2096004487$, we can compute $2^{n-1} \equiv 1992692247 \pmod{n}$. Hence n is composite. This does not tell much about how to factor it however.

There are some composite numbers which pass this test for all choices of a which are relatively prime to n. Such numbers are called **Carmichael** numbers. They are much less common than primes. For example, Erdös showed that the sum of their reciprocals converges. However, recent results have shown that they are nevertheless quite plentiful. An example is $n = 561 = (3)(11)(17)$. Notice that if $\gcd(a, 561) = 1$,

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{35} \equiv 1 \pmod{17} \end{aligned}$$

By the Chinese Remainder Theorem, one sees that $a^{560} \equiv 1 \pmod{561}$ for all a relatively prime to 561. In fact, a^{80} would suffice.

Still, without any additional computation, it is possible to improve this test. In our example, $560 = 16(35)$. Consider the computations

$$\begin{aligned} & & 2^{35} &\equiv 263 \pmod{561} \\ 2^{70} &= \left(2^{35}\right)^2 &&\equiv 166 \pmod{561} \\ 2^{140} &= \left(2^{70}\right)^2 &&\equiv 67 \pmod{561} \\ 2^{280} &= \left(2^{140}\right)^2 &&\equiv 1 \pmod{561} \\ 2^{560} &= \left(2^{280}\right)^2 &&\equiv 1 \pmod{561} \end{aligned}$$

We see from this sequence of equations that 67 is a square root of 1 modulo 561. If 561 were a prime, there would be only two square roots, namely ± 1. So this shows conclusively that 561 is composite. In this case however, information about the factors is revealed because

$$0 \equiv 67^2 - 1 = (67-1)(67+1) \pmod{561}.$$

So $\gcd(66, 561) = 33$ and $\gcd(68, 561) = 17$ are factors of 561.

The general procedure, known as the Miller-Rabin test, uses this approach. Moreover, it does not involve any more computation than it requires to get $a^{n-1} \pmod{n}$. Pull out all factors of 2 from $n-1$, say $n-1 = 2^d m$.

Now compute $a^m \pmod n$, and then successively square it to compute $a^{2m} \pmod n$, $a^{4m} \pmod n$, $a^{8m} \pmod n$,..., $a^{n-1} \pmod n$. If 1 does not occur in this list, then n fails our earlier primality test. However, if $a^{n-1} \equiv 1 \pmod n$ and $a^m \not\equiv 1 \pmod n$, then there is a last congruence in this list which is not 1. This will be a square root of 1 in $\mathbb{Z}_n$. If it is not -1, then n is definitely composite. This is because $x^2 = 1$ has only the solutions $x = \pm 1$ in a field, but can have more solutions when n is composite.

It is also easy to check whether n has any small prime factors. The computer can store the product P of all primes less than 1000. Compute $\gcd(n, P)$. If this is not 1, then n is composite. The composite numbers which pass the Miller-Rabin test for half a dozen random choices of a are quite rare. Indeed, a large number n which passes this test and has no small prime factors is almost surely prime. Such numbers have been called industrial grade primes. They are likely to be very hard to factor.

Exercises

1. Recall that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is a positive integer. Prove that if $n \geq 2$, then n is prime if and only if $\binom{n}{k} \equiv 0 \pmod n$ for all $1 \leq k \leq n-1$. This result plays an important role in the Agrawal-Kayal-Saxena algorithm.

2. Show that 3053 is not prime by finding a congruence identity that contradicts primality. Do not factor it.

3. Show that 3876721 is not prime by finding a congruence identity that contradicts primality. Do not factor it.

4. Show that 1729 is a Carmichael number. Find a congruence identity that proves that n is not prime. (A factorization of n is **not** a satisfactory substitute.)

5. Show that 5755495201 is a Carmichael number. Find a congruence identity which proves that n is not prime. (A factorization of n is **not** a satisfactory substitute.) You may use computer software.

6. Show that if $p = 6k + 1$, $q = 12k + 1$, and $r = 18k + 1$ are all prime, then pqr is a Carmichael number.

7. Korselt showed that a composite integer n is a Carmichael number if and only if it is square free and for every prime $p|n$, one has $(p-1)|(n-1)$. Prove that if n has this form, then it is a Carmichael number.

4.4. Factoring Algorithms

If you wish to factor a large number using a computer, there are various tricks you can try. No method known today can factor the product of two primes with 200–300 digits before the end of the universe. Nevertheless,

methods and computers will continue to improve. However, experts feel that it will always be significantly easier to find large primes than to factor the product of two of them. So the security of our code is guaranteed if we make our primes stay ahead of the factoring game.

However, most random numbers have small prime factors as well as large ones. Any sensible factoring algorithm starts by taking the gcd of n with the product of the first few primes. In this way, all factors less than, say 1000, may be pulled out. Then test what is left to see if it is composite. If it seems prime, it almost surely is. So now you try to prove that it is prime. If it is composite, the hard work begins. Unfortunately, it is known that on average, numbers do not have very many factors (relative to their size). So most factors are very big.

Most factoring schemes use quite sophisticated mathematics. Here is an elementary idea that goes back to Lagrange. The idea is simple: try to find non-trivial solutions of

$$x^2 \equiv y^2 \pmod{n}.$$

By non-trivial solution, we mean $x \not\equiv \pm y \pmod{n}$. If n is composite, say $n = ab$, then the solutions of

$$\begin{aligned} x - y &\equiv a \pmod{n} \\ x + y &\equiv b \pmod{n} \end{aligned}$$

provide non-trivial solutions. Conversely, if x and y form a non-trivial solution, then $\gcd(x \pm y, n)$ yield proper factors of n.

Lenstra and Pommerance have added some important new ideas to this method. They hope that it will prove to be a better method than others presently known. Their plan is to look for solutions of $x \equiv y \pmod{n}$ so that x and y are both products of only small primes. If enough solutions are found, they can be used to construct a solution of $x^2 \equiv y^2 \pmod{n}$. Let us illustrate this with a small example.

Let $n = 493$. A few trials yield the following equivalences $\pmod{493}$.

$$\begin{aligned} -3 &\equiv 490 = 2 \cdot 5 \cdot 7^2 \\ 7 &\equiv 500 = 2^2 \cdot 5^3 \\ 32 &\equiv 525 = 3 \cdot 5^2 \cdot 7 \\ -7 &\equiv 486 = 2 \cdot 3^5 \end{aligned}$$

All of these equations contain only powers of -1, 2, 3, 5, and 7. Using only the total parity of the exponents, we can represent these equations by vectors. For example, the first equation has one $-$ sign, and odd powers of 2, 3, and 5; but an even power of 7. This yields the vector $(1, 1, 1, 1, 0)$. Altogether we obtain

$$\begin{gathered} (1, 1, 1, 1, 0) \\ (0, 0, 0, 1, 1) \\ (0, 1, 1, 0, 1) \\ (1, 1, 1, 0, 1) \end{gathered}$$

In order to get squares, we wish to combine them so that all the parities are even. Combining the first, second and fourth achieves this. Multiplying the

three equations together yields

$$3 \cdot 7^2 \equiv 2^4 \cdot 3^5 \cdot 5^4 \cdot 7^2.$$

Cancellation yields $1 \equiv 2^4 3^4 5^4$. This provides a solution to $x^2 \equiv y^2$ with $x = 1$ and $y = 900$. Computing $\gcd(493, 901) = 17$ and $\gcd(493, 899) = 29$ provides a complete factorization.

Exercises

1. Use computer software to find enough congruences to factor 1643 by the method described in this section.

2. **(Factoring algorithms and primality testing)** Using computer software commands for the gcd and mod, but not a complete factoring command, interactively factor $n = 217601977016409565782951 60$, and report on the steps as you go along.

(i) Test for prime factors up to 1000 and factor them out. Let the large factor remaining be called m.

(ii) Compute $3^{m-1} \pmod{m}$. What does this tell you?

(iii) One must use a brute force method to factor m. You may use that 999983 is a factor. Let the other factor be called q.

(iv) Repeat (i) for $q - 1$. This yields a prime factorization. Why?

(v) Prove that q is prime by finding a primitive root, say r.

Notes on Chapter 4

The use of codes for the purpose of secure transfer of information has a long history. The primary uses were for military and political purposes, at least initially, as these parties had great resources. During World War II, codemaking and codebreaking were crucial parts of the war effort. This was the beginning of the use of calculating machines, and led to the computer revolution. The advent of computers has made the need for security in the transmission of messages something that is of importance to all of us.

Computers also provided the means to use more sophisticated methods both for encryption and the breaking of these codes. A central issue was always how two parties could share information about a code that was safe from prying eyes. A major breakthrough was made by Diffie, Hellman and Merkle [**10**] which allowed a public exchange between two parties to agree on a common key without revealing it to any eavesdropper. Diffie proposed that one could develop an asymetrical code with a public key for encryption that only the constructor could decode. This was accomplished by Rivest, Shamir and Adleman [**32**] at MIT in 1978. It has since come out that the codebreaking division of GCHQ, the British signals intelligence agency, came up with a similar method to that of Diffie-Hellman-Merkle almost a decade

earlier, but it was kept secret until recently. Since then, other methods have been developed for public key codes.

Simon Singh's book [**36**] is an interesting, non-technical introduction to codes and codebreaking.

The use of codes to allow for accurate transmission over noisy signals goes back to work of Hamming [**16**] in 1950. Nowadays, when large data files such as computer operating systems and other software are routinely downloaded over the internet, the accuracy of transmission becomes as important as security.

Computing the list of prime numbers goes back to ancient times. However the testing of large integers to decide if they are prime, primality testing, is a modern idea relying on computers. The Miller-Rabin test [**26**, **29**] dates from the mid-1970's. The first definitive algorithm to test for primality is due to Agrawal, Kayal and Saxena [**1**]. Charmichael numbers were introduced by Charmichael in 1910. There are infinitely many such numbers [**3**], but the sum of their reciprocals is finite [**11**]; so they are rare compared to prime numbers.

Factoring of composite numbers is considered to be very difficult, which is why the RSA scheme is thought to be secure. The modification of Lagrange's ideas from Section 4.4 is due to Lenstra and Pomerance [**23**]. The possibility of quantum computers and an algorithm of Peter Shor [**33**] would make factoring practical, and would break the RSA code. Other algorithms for encryption that are secure against quantum computation have been developed, but are not yet in widespread use.

Chapter 5

Real and Complex Numbers

In this chapter, we will learn about the fields of real and complex numbers. In particular, we will prove the famous Fundamental Theorem of Algebra which asserts that every polynomial with complex coefficients factors into a product of linear terms.

5.1. Real Numbers

We learn in calculus that the rational numbers are not sufficient for the study of functions. For example, a nice function like x^2-2 does not have any zeros if it is only defined on the rationals. Nor, from the point of view of algebra, are the rationals adequate because this polynomial does not factor. The 'natural' domain of this function should include $\sqrt{2}$. Similarly, the function x^4-8x does not achieve its minimum value at any rational number. It also turns out that the study of simple differential equations like $y'=y$ leads to the solution $f(x)=e^x$ where e is an even stranger 'number'. Similarly, the integral

$$\int_1^x \frac{1}{t}\,dt = \ln(x)$$

introduces another trancendental function, meaning a function that does not satisfy an algebraic equation. Of course, you have already learned about the trigonometric functions $\sin(x)$, $\cos(x)$, and so on which rely on the magic number π. So for various reasons, we find that the rational numbers are inadequate for the analysis of functions.

The answer is to allow these other 'numbers' which seem called for to fill the gaps between the rationals. There are a number of ways to define what these **real** numbers $\mathbb{R}$ should be. One of the simplest descriptions is to make use of the decimal system. We describe the set of real numbers as all possible *infinite* decimal expansions:

$$x = a_k a_{k-1} \dots a_1 a_0 . a_{-1} a_{-2} a_{-3} \dots$$

where a_i belong to the set $\{0,1,2,3,4,5,6,7,8,9\}$. Such expansions are already familiar for rational numbers such as $\frac{1}{3} = 0.33333\dots$ and $\frac{22}{7} =$

3.14285714 . . .. Every such expansion gives us a real number. One problem with this definition is that different decimal expansions may yield the same *number*. For example,

$$1.000\ldots = 0.999\ldots.$$

This is a fairly minor problem, but you have to deal with this ambiguity of names whenever you talk about the operations of addition, multiplication, inverses, and even equality. A more important problem with this definition is that it assumes implicitly that all of these symbols represent a number and that we can define addition and multiplication. If we consider them as infinite series, then that helps define these operations as limits, but the whole notion of limits creates new issues.

The discovery of the nature of the real numbers was intimately connected with the search for a good understanding of convergence and of the nature of sets. All these notions were formalized in the middle of the nineteenth century. See Manheim [**25**] for a history of topology. There were two different approaches.

Bolzano and later Cauchy introduced the notion of a **Cauchy sequence**, which is the criterion used to decide if a sequence is convergent *without* the need for any mention of the limit point itself. So one can consider the set of all possible 'limits' of sequences of rational numbers. For example, the sequence $e_n = \sum_{k=0}^{n} \frac{1}{k!}$ can be shown to converge very rapidly to the real number e. Even though e does not belong to the rational numbers, we can manipulate it in the same way by using these rational approximations. We are able to extend the notion of addition and multiplication because these operations are continuous.

We have omitted an important part of the definition. For each real number, there are many different convergent sequences with it as a limit. So in reality, one must put an equivalence relation on the set of Cauchy sequences. Two sequences are equivalent if they have the same limit. But since all this must be done without reference to a limit point, say that two Cauchy sequences $\{u_n\}$ and $\{v_n\}$ are equivalent if the sequence u_1, v_1, u_2, $v_2, \ldots$ is also a Cauchy sequence. Alternatively, two Cauchy sequences are equivalent if $\lim_{n\to\infty} u_n - v_n = 0$. The real numbers are the set of equivalence classes of Cauchy sequences of rational numbers. Each rational number r corresponds to the class containing the constant sequence $\{r, r, r, \ldots\}$.

Another solution was proposed by Dedekind. He suggested a more algebraic approach. Consider all proper subsets $A \subset \mathbb{Q}$ such that A has no largest element and if $a \in A$ and $b < a$, then $b \in A$. These objects are called Dedekind 'cuts', because they correspond to cutting the rational numbers into two at some 'real' point. For example,

$$A = \{r \in \mathbb{Q} : r \leq 0 \ \text{ or } \ r^2 < 2\}$$

represents $\sqrt{2}$. Addition can be defined on the sets themselves:

$$A + B := \{r + s : r \in A,\ s \in B\}.$$

Multiplication requires a little more ingenuity (try to define it), but is done in a similar manner. One may then verify all the axioms of a field.

We will not carry out the construction of the real numbers in this book. This discussion is for the purpose of making you aware that there were some significant problems involved in the definition of the real numbers that took many years to resolve. It took about 2000 years, from the Pythagorean school to the middle 1800's, to realize that one needed an abstract, non-geometric, definition of real numbers.

The real numbers have an important completeness property. This property was known before the real numbers were properly defined. Indeed, it was the realization that one needed to prove this completeness property that led to the more modern approach to mathematical proof. One way of stating this property is known as the:

5.1.1 Least upper bound property. *If X is a non-empty set of real numbers with an upper bound, then there is a least upper bound s. That is, every $a \in X$ satisfies $a \leq s$; and if every $a \in X$ satisfies $a \leq t$, then $s \leq t$.*

Let us look at how one can prove this using Dedekind's definition. Each $x \in X$ corresponds to a cut A_x. Define $S = \bigcup_{x \in X} A_x$. Let us now verify that S is a cut which represents the least upper bound s of X. Note that S is a proper subset of $\mathbb{Q}$ because it has an upper bound. If $a \in S$, then there is some $x_0 \in X$ so that $a \in A_{x_0}$. Hence any $b < a$ belongs to A_{x_0} and thus to S; and there is some $c \in A_{x_0} \subset S$ with $a < c$. Thus S is a cut. Now S is an upper bound for X because S contains A_x for each $x \in X$, and thus $x \leq s$ for all $x \in X$. On the other hand, if $x \leq t$ for all $x \in X$ and t is represented by a cut T, then T must contain A_x for every $x \in X$. Hence $S \subset T$, and therefore $s \leq t$.

The least upper bound property can be used to prove other basic properties of the real numbers. For example, the Intermediate Value Theorem and the fact that every Cauchy sequence of real numbers converges to a real number. This latter property is known as **completeness**. Other well known theorems such as the Heine-Borel Theorem and the Extreme Value Theorem depend crucially on this completeness property. We will require the Extreme Value Theorem in our proof of the Fundamental Theorem of Algebra. This is usually proven in a course on calculus or real analysis.

Exercises

1. Define multiplication using Dedekind's definition of the real numbers. HINT: do it first for two positive numbers.

2. Show that the associative law for addition holds in $\mathbb{R}$ using Dedekind cuts.

3. Prove the Intermediate Value Theorem: If f is a continuous function on $[0,1]$ such that $f(0) < 0$ and $f(1) > 0$, then there is a real number s such that $f(s) = 0$.
HINT: use the $\{x : f(x) < 0\}$ to help define a Dedekind cut.

4. Prove that every polynomial of odd degree with real coefficients has a real root.

5. As discussed in this section, $\mathbb{R}$ is constructed from $\mathbb{Q}$ by taking limits with respect to the absolute value. In this exercise we discuss another type of absolute value one may construct on $\mathbb{Q}$ that depends on a choice of prime p. One can also take limits of rational numbers with respect to this so-called p-adic norm and the result is a field known as the p-adic numbers.

Let p be a prime. Let $|0|_p = 0$. For any $0 \neq a \in \mathbb{Z}$, let $|a|_p = p^{-k}$, where $a = p^k u$ with $k \geq 0$ and $u \in \mathbb{Z}$ is relatively prime to p. For any $0 \neq q \in \mathbb{Q}$, write $q = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ non-zero and $\gcd(a,b) = 1$. Then let $|q|_p = |a|_p |b|_p^{-1}$.
(a) Prove that for all $q, r \in \mathbb{Q}$ we have $|qr|_p = |q|_p |r|_p$ and

$$|q + r|_p \leq \max\{|q|_p, |r|_p\} \leq |q|_p + |r|_p.$$

Show that $|q + r|_p = \max\{|q|_p, |r|_p\}$ if $|q|_p \neq |r|_p$.
(b) Prove that the following series converges with respect to $|\cdot|_p$

$$\sum_{n=0}^{\infty} p^n = -\frac{1}{p-1};$$

i.e., show that $\lim_{m\to\infty} \left|1 + (p-1)\sum_{n=0}^{m} p^n\right|_p = 0$.

5.2. Complex Numbers

From the point of view of algebra, the real numbers still are deficient. One would like to be able to completely factor all polynomials. But a polynomial like $x^2 + 1$ has no real roots. The solution is to invent a root which we call i. In other words, one constructs a larger number system which contains an element i such that $i^2 = -1$. Nothing prevents us from introducing such a symbol as long as we verify that our new system makes sense.

Define the set of **complex numbers** $\mathbb{C}$ to be the collection of all 'numbers' of the form $a + ib$ where a and b are real. It is often convenient to associate the number $a + ib$ with the vector (a, b) in the plane $\mathbb{R}^2$. Addition is defined by vector addition:

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

Multiplication is defined by extending real multiplication using the distributive law and the identity $i^2 = -1$. This forces the rule:

$$(a + bi)(c + di) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc).$$

5.2.1. Theorem. *The complex numbers form a field. That is, addition is commutative and associative, has the zero element* $0 = 0 + i0$*, and additive inverses* $-(a + ib) = (-a) + i(-b)$*. Multiplication is commutative and associative and distributes over addition, has the identity element* $1 = 1 + i0$*, and non-zero elements have (multiplicative) inverses.*

The proof of this theorem will not be written out in detail. A few comments will suffice here. The interested reader can carry out the rest of the argument. First, the properties of addition are valid because they are valid for vector addition. Commutativity of multiplication follows directly from the definition and commutativity of real multiplication. The associative law is a simple computation. Distributivity is also a routine computation. We will carry it out in detail to give the flavour of the proofs.

Let $u = a + ib$, $v = c + id$ and $w = e + if$ be three complex numbers. We have to verify the identity $(u + v)w = uw + vw$. Compute:

$$\begin{aligned}(u + v)w &= ((a + c) + i(b + d))\,(e + fi)\\ &= (ae + ce - bf - df) + i(af + cf + be + de)\\ &= ((ae - bf) + i(af + be)) + ((ce - df) + i(cf + de))\\ &= uw + vw\end{aligned}$$

The astute reader may notice that a special case of the distributive law is used in the proof. Multiplication by i does distribute over multiplication and addition of real numbers. This follows from the definition of complex addition and multiplication, and is not a circular proof.

Multiplicative inverses are worth investigating more closely. First, define the **complex conjugate** of a complex number $z = x + iy$ by $\overline{z} = x - iy$. Notice that $z\overline{z} = x^2 + y^2$ is a non-negative real number which is strictly positive except when $z = 0$. So it follows that

$$z^{-1} = \frac{\overline{z}}{z\overline{z}} = \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}.$$

This verifies all the properties of a field for $\mathbb{C}$.

Let us collect together some simple properties of the conjugate function. All of these properties are are left to the reader.

5.2.2. Proposition. *Complex conjugation is an involution that preserves all the field operations:*

(1) *Involution:* $\overline{\overline{z}} = z$.
(2) *Addition:* $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
(3) *Multiplication:* $\overline{(z_1 z_2)} = \overline{z_1}\,\overline{z_2}$.

There is an important geometric interpretation of the quantity $z\overline{z} = x^2 + y^2$. This represents the square of the Euclidean length of the vector (x, y) in the plane. So one introduces the notion of **absolute value** or **modulus** for $z = x + iy$:

$$|z| = (z\overline{z})^{1/2} = \sqrt{x^2 + y^2}.$$

We also introduce the real and imaginary parts of $z = x + iy$ defined by

$$\operatorname{Re} z = x = \frac{z + \overline{z}}{2} \qquad \operatorname{Im} z = y = \frac{z - \overline{z}}{2i}.$$

The following proposition summarizes the basic properties of absolute value.

5.2.3. Proposition. *Let $z = x + yi$ and $w = u + vi$ be two complex numbers. Then*

(1) $|\overline{z}| = |z|$.
(2) $|zw| = |z|\,|w|$.
(3) $|z| \geq 0$. *Moreover,* $|z| = 0$ *implies that* $z = 0$.
(4) $|\operatorname{Re} z| \leq |z|$ *and* $|\operatorname{Im} z| \leq |z|$.
(5) (*Triangle Inequality*) $|w + z| \leq |w| + |z|$.

Proof. The proofs of (1) and (3) are routine. For (2), notice that

$$|zw|^2 = zw\overline{zw} = z\overline{z}w\overline{w} = |z|^2|w|^2.$$

Property (4) is immediate from

$$|z|^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2.$$

Finally, the most important property is the triangle inequality. This name comes from the fact that the vectors w, z, and $w + z$ form the three sides of a triangle. The triangle inequality states that the length of one side is no longer than the sum of the lengths of the other two sides.

$$\begin{aligned} |w + z|^2 &= (w + z)(\overline{w} + \overline{z}) \\ &= w\overline{w} + w\overline{z} + z\overline{w} + z\overline{z} \\ &= |w|^2 + 2\operatorname{Re}(w\overline{z}) + |z|^2 \\ &\leq |w|^2 + 2|w\overline{z}| + |z|^2 \\ &= |w|^2 + 2|w|\,|z| + |z|^2 = (|w| + |z|)^2. \end{aligned}$$

Taking square roots establishes the inequality. ■

In Chapter 7, we introduce a general method for building a larger field in which a given irreducible polynomial has a root. In this language, we will see that starting with $\mathbb{R}$ and the polynomial $x^2 + 1$, we construct a field isomorphic to $\mathbb{C}$ by adding a root i of $x^2 + 1$.

Exercises

1. Prove that $|w - z| \geq |w| - |z|$ for all complex numbers w and z.

2. Show that z and z^{-1} lie on a straight line through 0.
Show that if $w \in \mathbb{C}$ is a root of a polynomial $p(x)$ with real coefficients, then $p(\overline{w}) = 0$ as well.

3. Prove that one cannot define an order $<$ on the field of complex numbers (see properties [O1] and [O2] from Section 1.1).

4. Show that there is no intermediate value theorem for polynomials with complex coefficients.

5. **(Products of sums of two squares)** Use complex numbers to prove that if $a, b, c, d \in \mathbb{Z}$, then there exist $x, y \in \mathbb{Z}$ such that $(a^2 + b^2)(c^2 + d^2) = x^2 + y^2$. (Compare with Lemma 3.5.5.)

6. Show that the set S of 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ form a field under matrix addition and multiplication. Prove that the map

$$\varphi\colon \mathbb{C} \to S, \qquad \varphi(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

is an isomorphism of fields.

7.★ If you are familiar with the properties of determinants, use the representation of the complex numbers in Exercise 6 to prove that $|wz| = |w||z|$ by computing the determinants of the corresponding matrices.

5.3. Polar Form

Every point in the plane can be described by its Cartesian coordinates (x, y). It can also be described by its **polar coordinates**, (r, θ), where $r = (x^2 + y^2)^{1/2}$ is the length of the vector (x, y) and θ is the (oriented) angle in radians between the positive real axis and the ray determined by positive multiples of the vector (x, y). The Cartesian coordinates are determined from the polar form by the equations

$$x = r\cos(\theta) \quad \text{and} \quad y = r\sin(\theta).$$

Conversely, the polar coordinates are obtained from the Cartesian form by solving these equations. Of course, the angle θ is determined only up to a multiple of 2π.

This can be applied to the complex plane via its identification with $\mathbb{R}^2$. The **argument** of a complex number $z = x + iy$ is the angle $\mathrm{Arg}(z) = \theta$ in the polar form (r, θ) of the vector (x, y). Again, this argument is only determined as a real number modulo 2π. Of course, $r = |z|$. Let us introduce

a notation which will be used *only* for the next two sections:

$$\operatorname{cis}(\theta) := \cos(\theta) + i\sin(\theta).$$

This complex number lies on the circle of radius 1, centre 0, known as the unit circle. Conversely, every point on the unit circle has this form. So every complex number can be represented as $z = r\ \operatorname{cis}(\theta)$. The significance of this is that the argument of a product is the sum of the arguments.

5.3.1. Proposition. $r_1 \operatorname{cis}(\theta_1)\, r_2 \operatorname{cis}(\theta_2) = (r_1 r_2) \operatorname{cis}(\theta_1 + \theta_2)$.

Proof. Calculate

$$\begin{aligned}\operatorname{cis}(\theta_1)\ \operatorname{cis}(\theta_2) &= (\cos(\theta_1) + i\sin(\theta_1))(\cos(\theta_2) + i\sin(\theta_2)) \\ &= \big(\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)\big) + i\big(\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)\big) \\ &= \cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2) = \operatorname{cis}(\theta_1+\theta_2).\end{aligned}$$

The fact that the absolute values multiply is a consequence of Proposition 5.2.3 (2). ■

An immediate consequence of this is known as **de Moivre's Theorem**.

5.3.2. Corollary. $(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$ *for* $n \geq 1$.

This formula is quite useful for calculations of certain sines and cosines. For example, consider this identity for $n = 5$.

$$\begin{aligned}\cos(5\theta) + i\sin(5\theta) &= (\cos(\theta) + i\sin(\theta))^5 \\ &= \big(\cos^5(\theta) - 10\cos^3(\theta)\sin^2(\theta) + 5\cos(\theta)\sin^4(\theta)\big) \\ &\quad + i\big(5\cos^4(\theta)\sin(\theta) - 10\cos^2(\theta)\sin^3(\theta) + \sin^5(\theta)\big)\end{aligned}$$

By using the identity $\cos^2(\theta) + \sin^2(\theta) = 1$, we obtain

$$\begin{aligned}\sin(5\theta) &= 5\left(1 - \sin^2(\theta)\right)^2 \sin(\theta) - 10\left(1 - \sin^2(\theta)\right)\sin^3(\theta) + \sin^5(\theta) \\ &= 16\sin^5(\theta) - 20\sin^3(\theta) + 5\sin(\theta)\end{aligned}$$

In particular, apply this when $\theta = \pi/5$. Then $\sin(\pi/5)$ is a root of the polynomial equation $16x^5 - 20x^3 + 5x = x(16(x^2)^2 - 20x^2 + 5) = 0$. Since $\sin(\pi/5) \neq 0$, it follows that $\sin^2(\pi/5)$ is a root of the quadratic equation

$$16y^2 - 20y + 5 = 0.$$

This equation has roots $\frac{5 \pm \sqrt{5}}{8}$. To decide which root equals $\sin(\pi/5)$, notice that $0 < \pi/5 < \pi/4$. Thus this angle lies in the first quadrant, on which $\sin(x)$ is monotone increasing. So

$$0 < \sin(\pi/5) < \sin(\pi/4) = 1/\sqrt{2}.$$

Clearly, $\dfrac{5-\sqrt{5}}{8} < \dfrac{1}{2} < \dfrac{5+\sqrt{5}}{8}$. So,

$$\sin(\pi/5) = \sqrt{\frac{5-\sqrt{5}}{8}}$$

$$\cos(\pi/5) = \sqrt{\frac{3+\sqrt{5}}{8}} = \frac{1+\sqrt{5}}{4}.$$

We can also solve other simple polynomial equations. For example, consider

$$z^4 + 4 = 0.$$

Writing $z = r\,\mathrm{cis}(\theta)$, the equation becomes

$$r^4\,\mathrm{cis}(4\theta) = -4 = 4\,\mathrm{cis}(\pi).$$

Hence $r = \sqrt{2}$ and θ is an angle such that $4\theta \equiv \pi \pmod{2\pi}$. So

$$\theta = \frac{\pi + 2k\pi}{4} = \frac{\pi}{4} + \frac{\pi}{2}k$$

for some integer k. Only the values $k = 0, 1, 2, 3$ are important, for after that, the values repeat modulo 2π. Hence the roots are

$$\begin{array}{rcccr} z_1 & = & \sqrt{2}\,\mathrm{cis}(\pi/4) & = & 1+i \\ z_2 & = & \sqrt{2}\,\mathrm{cis}(3\pi/4) & = & -1+i \\ z_3 & = & \sqrt{2}\,\mathrm{cis}(5\pi/4) & = & -1-i \\ z_4 & = & \sqrt{2}\,\mathrm{cis}(7\pi/4) & = & 1-i \end{array}$$

Exercises

1. Find the Cartesian form of all cube roots of $8i$.

2. Find the exact values of $\sin(\pi/12)$ and $\cos(\pi/12)$ by using the identity

$$\mathrm{cis}(\pi/3)\,\mathrm{cis}(-\pi/4) = \mathrm{cis}(\pi/12).$$

3. Find all complex roots of the polynomial $z^{10} + z^5 + 1 = 0$. Express at least one of them in Cartesian form.

4. Use de Moivre's theorem to obtain a formula for $\cos 4\theta$ and $\sin 4\theta$.

5. Find all the 6th roots of -1. Graph them on the plane.

6. Calculate $(1+i)^{2023}$.

7. Prove the quadratic formula for a quadratic with complex coefficients. Deduce that every quadratic in $\mathbb{C}[x]$ has two complex roots.
HINT: complete the square.

8. (a) Solve $z^4 + 16 = 0$.
(b) Hence factor $p(x) = x^4 + 16$ as a product of two *real* quadratic polynomials.

5.4. The Exponential Function

In this section, we will extend the definition of the exponential function to all complex numbers. To do this, we will search for a differentiable function $E : \mathbb{C} \to \mathbb{C}$ such that $E(w + z) = E(w)E(z)$ for all w and z in $\mathbb{C}$ and $E(x) = e^x$ for all $x \in \mathbb{R}$. Once we have established the existence of this function, we will write e^z for $E(z)$.

Let us calculate some simple properties that such a function must have. First,

$$E(x + iy) = e^x E(iy).$$

And using the differentiability, we get

$$\begin{aligned} E'(z) &= \lim_{h\to 0} \frac{E(z+h) - E(z)}{h} \\ &= E(z) \lim_{h\to 0} \frac{E(h) - E(0)}{h} \\ &= E(z) \lim_{x\to 0} \frac{e^x - 1}{x} = E(z). \end{aligned}$$

Equality from line 2 to line 3 follows because we have assumed that the first limit exists.

Now concentrate on the function $f(y) = E(iy)$. Split it into its real and imaginary parts as $f(y) = E(iy) = A(y) + iB(y)$. Differentiating with respect to y yields

$$\begin{aligned} f'(y) &= A'(y) + iB'(y) \\ &= E'(iy)\frac{d(iy)}{dy} \\ &= iE(iy) = -B(y) + iA(y) \end{aligned}$$

So we arrive at the system of differential equations

$$\begin{aligned} A'(y) &= -B(y) \\ B'(y) &= \quad A(y). \end{aligned}$$

This leads to the second order differential equation $A''(y) = -A(y)$. From the identity $1 = E(0) = A(0) + iB(0)$, we also get the *initial conditions* $A(0) = 1$ and $A'(0) = -B(0) = 0$. From calculus, we know that this system has a unique solution $A(y) = \cos(y)$ and $B(y) = \sin(y)$.

Thus we arrive at a unique solution $E(iy) = \cos(y) + i\sin(y) = \operatorname{cis}(y)$. So

$$E(x + iy) = e^x(\cos(y) + i\sin(y)) = e^x \operatorname{cis}(y).$$

For this reason, we will usually write $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ instead of $\operatorname{cis}(\theta)$ from now on.

Let us verify that this function indeed has the properties that we searched for.

$$\begin{aligned} E(x+iy)E(u+iv) &= e^x \operatorname{cis}(y) e^u \operatorname{cis}(v) \\ &= e^{x+u} \operatorname{cis}(y+v) = E((x+iy)+(u+iv)). \end{aligned}$$

So E satisfies the multiplicative property.

The derivative property is a bit more delicate. The hard part is to show that $E'(0) = 1$. For then, as above, we obtain

$$E'(z) = E(z)E'(0) = E(z).$$

To verify that $E'(0) = 1$, we must show that

$$\lim_{h \to 0} \frac{|E(h) - 1 - h|}{|h|} = 0.$$

The complication comes from the fact that h takes all small *complex* values, not just real values, as it approaches 0. However, we need only facts from the calculus of real functions to verify this limit. The major tool for making estimates is the mean value theorem. Let us write $h = x + iy$, so that

$$|h| = \sqrt{x^2 + y^2}.$$

We may assume that $|h| < 1$, so in particular, $|x| < 1$. Calculate

$$\begin{aligned} E(h) - 1 - h &= e^x \cos(y) + ie^x \sin(y) - 1 - x - iy \\ &= e^x(\cos(y) - 1) + (e^x - 1 - x) + ie^x(\sin(y) - y) + iy(e^x - 1) \end{aligned}$$

Each of these terms can be estimated by the mean value theorem. First, since $f(y) = \cos(y)$ has derivative $f'(y) = -\sin(y)$, it follows that there is a value c between 0 and y such that

$$\begin{aligned} |\cos(y) - 1| &= |f(y) - f(0)| \\ &= |f'(c)||y| = |-\sin(c)||y| \le |c||y| \le |y|^2. \end{aligned}$$

So $e^x|\cos(y) - 1| \le e|y|^2 \le e|h|^2$ provided that $|x| \le 1$.

A similar treatment of the function e^x shows that $|e^x - 1| \le e|x|$ for $|x| \le 1$. Now repeat the argument for the function $g(x) = e^x - 1 - x$, which has derivative $g'(x) = e^x - 1$. Again by the mean value theorem, there is a point c between 0 and x so that

$$\begin{aligned} |e^x - 1 - x| &= |g(x) - g(0)| = |xg'(c)| \\ &= |x||e^x - 1| \le e|x|^2 \le e|h|^2. \end{aligned}$$

A third application with the function $h(y) = \sin(y) - y$ and derivative $h'(y) = \cos(y) - 1$ yields a point c between 0 and y so that

$$|\sin(y) - y| = |y||\cos(c) - 1| \le |y||c|^2 \le |y|^3.$$

Together with the inequality $|e^x| \le e$ for $|x| \le 1$ yields

$$|ie^x(\sin(y) - y)| \le e|y|^3 \le e|h|^3.$$

Finally, the fourth term is handled by $2|xy| \leq x^2 + y^2 = |h|^2$, so

$$|y(e^x - 1)| \leq e|y||x| \leq 2|h|^2.$$

Putting it all together yields, for $|h| \leq 1$,

$$|E(h) - 1| \leq e|h|^2 + e|h|^2 + e|h|^3 + 2|h|^2 = (2e + 2 + e|h|)|h|^2.$$

Thus

$$\lim_{h \to 0} \frac{|E(h) - 1 - h|}{|h|} = 0.$$

Exercises

1. (a) Graph the image of a line parallel to the y-axis under the exponential map.
(b) Graph the image of a line parallel to the x-axis under the exponential map.
(c) Show that the strip $\{z = x + iy : 0 \leq y < 2\pi\}$ is mapped by the exponential function one to one and onto the whole complex plane.

2. **(Sum Angle Formula for** sin **and** cos**)** Use the formulae $\cos(z) = (e^{iz} + e^{-iz})/2$ and $\sin(z) = (e^{iz} - e^{-iz})/2i$.
(a) Prove that $\sin(w + z) = \sin(w)\cos(z) + \cos(w)\sin(z)$.
(b) Prove that $\cos(w + z) = \cos(w)\cos(z) - \sin(w)\sin(z)$.

3. Find all solutions of $\sin(z) = 2$.

4. Let $f(z) = w_1 \sin(z) + w_2 \cos(z)$, where $w_1, w_2 \in \mathbb{C}$. Compute $f''(z)$.

5.5. Fundamental Theorem of Algebra

In this section, we will prove the famous Fundamental Theorem of Algebra that states that every polynomial with complex coefficients factors into a product of linear terms. It is not easy to prove this theorem in a strictly algebraic way. Indeed, one can argue that it is really the analytic properties of polynomials that make this result transparent. There are several accessible proofs. They all rely on some property of functions that depends on the completeness properties of the real and complex numbers. This proof depends on the Extreme Value Theorem: *a continuous real valued function on a closed bounded subset of the plane achieves its maximum value at some point.* If you have only seen this for functions on an interval, see Exercise 4.

We begin with a preliminary lemma.

5.5.1. Lemma. *Let $\mathbb{F}$ be a field and assume that every polynomial with coefficients in $\mathbb{F}$ has a root in $\mathbb{F}$. Then every polynomial with coefficients in $\mathbb{F}$ of degree $d \geq 1$ factors into a product of d linear terms.*

Proof. We will use induction on the degree d of polynomial with coefficients in $\mathbb{F}$. For $d = 1$, the result is clear. Now for $d > 1$, if p is a polynomial of degree d, by hypothesis it has a root $r \in \mathbb{F}$. So, $p(z) = (z - r)q(z)$ with q a degree $d - 1$ polynomial. By the induction hypothesis, $q(z)$ factors as a product of $d-1$ linear factors. Hence $p(z)$ factors as the product of d linear factors. ■

5.5.2 Fundamental Theorem of Algebra. *Every polynomial with complex coefficients of degree $d \geq 1$ factors into a product of d linear terms.*

Proof. Let $p(z) = \sum_{i=0}^{d} a_i z^i$ be a polynomial of degree $d \geq 1$; so that $a_d \neq 0$. By Lemma 5.5.1, it is enough to show p has a complex root. Assume, to the contrary, that $p(z)$ is never 0. In particular $a_0 = p(0) \neq 0$.

The proof will be divided into 3 main steps:

(1) Find a global minimum for $|p|$.
(2) Normalize p to obtain a polynomial q with $\min |q(z)| = 1 = q(0)$. Then we may write $q(z) = 1 + q_0(z)$.
(3) Show $q_0(z)$ achieves a small negative value, contradicting the fact that the minimum of q is 1.

A key point to observe here is that Steps 1 and 2 work over $\mathbb{R}$, so it is only in Step 3 where we make use of $\mathbb{C}$.

Step 1. Notice that

$$\lim_{|z|\to\infty} |p(z)| = \lim_{|z|\to\infty} |z|^d \left| a_d + \frac{a_{d-1}}{z} + \frac{a_{d-2}}{z^2} + \ldots + \frac{a_0}{z^d} \right| = \infty$$

since the second factor tends to the finite non-zero limit $|a_d|$ and $|z|^d$ tends to infinity. Thus there is a large real number R so that $|p(z)| > |a_0|$ for all $|z| > R$.

By the Extreme Value Theorem applied to the continuous real valued function $f(z) = -|p(z)|$ on the closed bounded set $\{z \in \mathbb{C} : |z| \leq R\}$, there is a point z_0 so that

$$|p(z_0)| \leq |p(z)| \quad \text{for all} \quad z \in \mathbb{C},\ |z| \leq R.$$

But for $|z| > R$, one has $|p(z)| > |a_0| = |p(0)| \geq |p(z_0)|$. So $|p(z)|$ achieves its global minimum at z_0.

Step 2. To simplify the computations, replace $p(z)$ by the polynomial

$$q(z) = \frac{p(z + z_0)}{p(z_0)}.$$

Notice that $q(z)$ is also a polynomial of degree d which is never 0, and $|q|$ takes its minimum value 1 at $z = 0$. That is,

$$1 = q(0) \leq |q(z)| \quad \text{for all} \quad z \in \mathbb{C}.$$

The constant term of q is 1. Let b be the next non-zero coefficient; so that

$$q(z) = 1 + bz^k + \text{higher order terms} = 1 + bz^k r(z)$$

where r is another polynomial such that $r(0) = 1$.

Step 3. Since $r(z)$ is continuous, there is a positive real number ε so that

$$|r(z) - 1| < \frac{1}{2} \quad \text{for} \quad |z| \leq \varepsilon.$$

Choose an angle θ so that $be^{ik\theta}$ is a negative real number. Indeed, one can take $\theta = -\operatorname{Arg}(b)/k$. Set $w = \varepsilon e^{i\theta}$, and note that because of the choice of θ, one has $bw^k = -|b|\varepsilon^k$. By replacing ε by an even smaller positive number if necessary, we can also suppose that $|bw^k| < 1$. Let us also write $r(w) = 1 + u$, where $|u| < \frac{1}{2}$. Therefore,

$$q(w) = 1 + bw^k r(w) = 1 - |b|\varepsilon^k(1 + u) = (1 - |b|\varepsilon^k) + |b|\varepsilon^k u.$$

Hence

$$|q(w)| \leq 1 - |b|\varepsilon^k + |b|\frac{\varepsilon^k}{2} = 1 - |b|\frac{\varepsilon^k}{2} < 1.$$

This contradicts the fact that q has minimum modulus 1. So the assumption that q and p have no roots is false. Hence p has a root. Therefore by Lemma 5.5.1, the proof is complete. ■

Exercises

1. Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_i \in \mathbb{C}$. Prove that every root α of f satisfies

$$|\alpha| \leq \max\Big\{1, \sum_{j=0}^{d-1} |a_j|\Big\}.$$

2. **(Cauchy's bound)** Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a monic polynomial, and let r be a root. Prove that $|r| \leq 1 + A$ where $A = \max\{|a_i| : 0 \leq i < n\}$.
HINT: if $|r| > 1$, use $r^n = -\sum_{i=0}^{r-1} a_i r^i$ to bound $|r|^n$.

3. **(Partial fraction decomposition)** Let f and g be polynomials with complex coefficients. We may write $g(x) = \prod_{i=1}^{n}(x - r_i)^{m_i}$ with $r_1, \ldots, r_n \in \mathbb{C}$ distinct. Prove that there is a polynomial $h(x)$ and constants $a_{ij} \in \mathbb{C}$ such that

$$\frac{f(x)}{g(x)} = h(x) + \sum_{i=1}^{n}\sum_{j=1}^{m_i} \frac{a_{ij}}{(x - r_i)^j}.$$

4.★ **(EVT for a rectangle)** Assume the Extreme Value Theorem for a continuous function on an interval $[a, b] \subset \mathbb{R}$, and prove it for a continuous function $f(x, y)$ on a rectangle $[a, b] \times [c, d]$.

HINT: for $x \in [a,b]$, let $f_x(y) = f(x,y)$ be a function on $[c,d]$. Find $y(x)$ so that f_x attains its maximum at $y(x)$. Let $g(x) = \max f_x$. Show that g is continuous on $[a,b]$.

5.★ Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbb{Z}$ and suppose that

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Let $z_1, \ldots, z_n \in \mathbb{C}$ be the roots of f. Prove there is a unique i such that $|z_i| > 1$, and $|z_j| < 1$ for all $j \neq i$. [1]

6.★ (Gershgorin Disc Theorem) Let $A = (a_{ij})_{1 \leq i,j \leq n}$ be an $n \times n$ matrix with the $a_{ij} \in \mathbb{C}$. For $1 \leq i \leq n$, let $R_i = \sum_{j \neq i} |a_{ij}|$. Let $\lambda \in \mathbb{C}$ be an *eigenvalue* of A, i.e., there exists an $n \times 1$ matrix $v \neq 0$ such that $Av = \lambda v$. Let

$$D(a_{ii}, R_i) = \{z \in \mathbb{C} : |z - a_{ii}| \leq R_i\},$$

known as a Gershgorin disc. Prove that λ lies in a Gershgorin disc.
HINT: pick i_0 so that $|v_{i_0}| = \max\{|v_i| : 1 \leq i \leq n\}$ and look at the i_0th coefficient of $Av - \lambda v$.

5.6. Real Polynomials

The theory for real polynomials is not quite as simple as for complex polynomials because certain real polynomials do not factor into real linear factors. However, we may use the Fundamental Theorem of Algebra to figure out what happens.

5.6.1. Lemma. *Let $p(x)$ be a polynomial with real coefficients. Then if a is a complex root of p, then $\overline{a}$ is also a root.*

PROOF. Let $p(z) = \sum_{i=0}^{d} p_i z^i$. This is immediate from the observation

$$p(\overline{a}) = \sum_{i=0}^{d} p_i \overline{a}^i = \sum_{i=0}^{d} \overline{p_i a^i} = \overline{p(a)} = 0. \qquad \blacksquare$$

5.6.2. Theorem. *Every real polynomial factors into a product of linear and quadratic factors, in which the quadratic factors have no real roots.*

Proof. By the Fundamental Theorem of Algebra, the polynomial p can be factored into linear complex terms. By factoring out the leading coefficient,

$$p(x) = c(x - a_1)(x - a_2)\ldots(x - a_d).$$

[1] This is due to Panaitopol. See `https://yufeizhao.com/olympiad/intpoly.pdf`.

Now c is real. Whenever a_i is real, $x - a_i$ is a factor of p over the real field. When a_i is not real, the lemma shows that there is an integer j so that $a_j = \overline{a_i}$. In this case, write $a_i = u + iv$ and $a_j = u - iv$. Then

$$(x - a_i)(x - a_j) = x^2 - 2ux + (u^2 + v^2).$$

This is a real polynomial.

It remains to show that all the roots come in pairs. This is seen by induction on the degree of p. Indeed, this is true for degree $d = 1$. If the result holds for all real polynomials of lower degree, consider the case for p above. If p has a real root a_1, then p factors as $p(x) = (x - a_1)p_1(x)$. Moreover, it is clear that division of p by $x - a_1$ uses only real coefficients. So p_1 is real. Similarly, if p has a pair of non-real roots $a_1 = u + iv$ and $a_2 = u - iv$, then p factors as $p(x) = (x^2 - 2ux + u^2 + v^2)p_1(x)$. Again, division of a real polynomial by another leaves a real quotient. In either case, the induction hypothesis applies to $p_1(x)$ and it factors as a product of linear terms and quadratic terms with non-real roots. Hence the result follows for p as well. ■

We get the following immediate corollary about real polynomials of odd degree because at least one of the factors must be of odd degree (hence degree 1). This is also an immediate consequence of the Intermediate Value Theorem.

5.6.3. Corollary. *A real polynomial of odd degree has at least one real root.*

Somehow we have managed all this discussion of factorization without any discussion of uniqueness. Of course, this is a crucial issue. Because the factorization over the real or complex numbers is intimately connected with roots, this question can be handled here by special ad hoc arguments. However, we will see in the next chapter that the polynomials over any field always have unique factorization into 'primes', known as irreducible polynomials.

Exercises

1. Show that a quadratic $p(x) = ax^2 + bx + c$ with real coefficients has two (possibly equal) real roots if and only if the discriminant $\Delta(p) = b^2 - 4ac$ is non-negative.

2. **(Partial fraction decompositions, again)** Let f and g be polynomials with real coefficients. Write $g(x) = \prod_{i=1}^{n}(x - r_i)^{m_i} \prod_{j=1}^{N} q_j(x)^{M_j}$ with $r_1 \ldots, r_n \in \mathbb{R}$ distinct and the $q_j(x)$ quadratic polynomials with no real roots. Prove that there is a polynomial $h(x)$, constants $a_{ik} \in \mathbb{R}$,

and linear polynonomials $\ell_{ik}(x) \in \mathbb{R}[x]$ so that

$$\frac{f(x)}{g(x)} = h(x) + \sum_{i=1}^{n} \sum_{k=1}^{m_i} \frac{a_{ik}}{(x-r_i)^k} + \sum_{j=1}^{N} \sum_{k=1}^{M_j} \frac{\ell_{ik}(x)}{q_j(x)^k}.$$

3. (Descartes's Rule of Signs) Let $p(x)$ be a polynomial with real coefficients. Write $p(x) = a_{i_1}x^{i_1} + \cdots + a_{i_m}x^{i_m}$ where $i_1 > i_2 > \cdots > i_m \geq 0$ and all $a_{i_j} \neq 0$. Let s be the number of sign changes in the coefficients of p, i.e., s is the total number of times for which $a_{i_j}a_{i_{j+1}} < 0$. Let t be the number of positive roots of p, counting multiplicity (e.g., a factor of $(x-r)^k$ counts as k roots). In this exercise, we prove that $t \leq s$ and $s - t$ is even.

(a) Reduce to the case in which $a_{i_1} = 1$ and $i_m = 0$.
(b) Using Calculus, show that if $a_{i_1}a_0 > 0$, then there are an even number of positive roots, and if $a_{i_1}a_0 < 0$, then there are an odd number of positive roots by comparing the behaviour of p near 0 and ∞.
(c) Conclude that $s - t$ is even.
(d) Let $r > 0$. Show that if $a_{i_j}a_{i_{j+1}} < 0$, then the coefficient of $x^{i_{j+1}+1}$ in $(x-r)p(x)$ agrees in sign with $a_{i_{j+1}}$.
(e) Combine these facts to show that the number and parity of the sign changes must increase when multiplying by $x - r$.
(f) Using induction on the number of positive roots, prove Descartes's Rule of Signs.

Notes on Chapter 5

A precise notion of the real and complex numbers as we know it is a rather modern idea. To the ancient civilizations, numbers were positive integers. (See the notes to Chapter 1.) Positive rationals were considered as ratios between two positive integers. The discovery that certain square roots such as $\sqrt{2}$ were not 'commensurable' with the integers was disturbing. Some, like the Babylonians, considered successive rational approximations of these numbers. Nevertheless, no notion of an extended number system developed at that time.

Stevin proposed the use of finite decimals to represent numbers in 1585. He recognized that arbitrary quantities could be approximated by his decimals. But since a value like $\frac{1}{3}$ did not have an exact representation, most others rejected the idea. Even 200 years later, Euler considered the real numbers as the set of all 'magnitudes', and apparently no definition was considered necessary. However Euler introduced the notion of a variable x which could take any magnitude. Since roots of equations were by this time known that may not be real, it raised the issue of what a real number was.

Bolzano, in 1817, had a notion of real numbers and completeness using Cauchy sequences of rationals; but never published. Cauchy also considered

the notion of convergent sequences of rationals, but did not propose a proper theory. In 1858, Dedekind published his theory of the reals using cuts. In 1869, Meray published a construction using Cauchy sequences. Weierstrass, Cantor and Heine also had related approaches. In 1900, Hilbert developed an axiomatic approach: axioms for an ordered field together with two critical axioms, the Archimedean property (there are no numbers x such that $0 < x$ and $x < \frac{1}{n}$ for all $n \geq 1$) and a completeness property. He established the uniqueness of such a field, thereby showing that different constructions such as Dedekind's and Meray's must yield identical objects.

Surprisingly quadratic equations did not lead to the discovery of complex numbers, because a simple check of the discriminant determines whether there are (real) solutions or not. In the early 1500's, del Ferro and Tartaglia found the formula for the roots of a cubic. This involved square roots of negative numbers even when the roots are real. Cardano, who found the formula for the roots of a quartic, considered numbers of the form $a + \sqrt{-b}$. He was not convinced that they were bona fide quantities, but they worked. Descartes, in 1637, coined the term 'imaginary number'. Euler introduced the use of $i = \sqrt{-1}$, as well as the polar form. Argand came up with the notion of representing complex numbers in the plane in 1806. In 1831, Hamilton described the complex numbers as ordered pairs of reals, (a, b), with vector sums and product $(a, b)(c, d) = (ac - bd, bc + ad)$. Gauss was aware of the geometric representation of complex numbers in 1796, but did not publish it until 1831. In 1847, Cauchy constructed the complex numbers as an extension of the reals, $\mathbb{R}[x]/(x^2 + 1)$. Cauchy was also responsible for the beginnings of complex function theory (calculus for complex valued functions).

The fundamental theorem of algebra was proposed by Roth and later Girard in the early 1600's, both stating that a (real) polynomial of degree n *may* have n roots. D'Alembert had a proof in 1746, but it had a gap. Euler, Lagrange and others made attempts, but implicitly assumed that there was a field extension in which the polynomial already has n roots. Wood in 1798 and Gauss in 1799 published proofs, that also had gaps. In 1806, Argand published the first rigorous proof. Moreover he was the first to allow complex coefficients for his polynomials. Gauss published two other proofs in 1816. The proof that we give uses the extreme value theorem. A proof of this was found by Bolzano in 1830, but never published. It was later proven by Weierstrass in 1860. The extreme value theorem depends on the completeness property of the real numbers.

Various introductory books on real analysis provide some construction of the real numbers. The uniqueness is more subtle. A treatment of both can be found in Garling [**12**, Ch.2-3]. The fundamental theorem of algebra is fundamentally a result in analysis. Standard comprehensive treatises on algebra usually assume that polynomials of odd degree have a real root. This is basically assuming the Intermediate value theorem, which is a consequence of the completeness of the reals. Other proofs using complex analysis can

be found in many texts; for example Simon [**35**] has three proofs. The proof given in our book is perhaps the simplest if one knows about the completeness of the real numbers.

Chapter 6

The Ring of Polynomials

In this chapter, we investigate the algebraic properties of polynomials. The reader should notice the parallels between the structure of the integers and the structure of the polynomials. Most of the ideas that have been developed for integers, such as primes, modular arithmetic, and so on, have a polynomial version.

6.1. Preliminaries on Polynomials

We use the notation $R[x]$ to denote the set of all polynomials with coefficients in a ring R. That is, an element of $R[x]$ is an expression of the form

$$r_d x^d + r_{d-1} x^{d-1} + \ldots + r_1 x + r_0$$

where x is a formal symbol and the coefficients r_i belong to R. In particular, we are especially interested in the case when R is a field. So we will use the symbol $\mathbb{F}$ whenever we mean the result works for any field. The fields of interest to us at the moment are the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the fields $\mathbb{Z}_p$ for p prime. So $\mathbb{F}[x]$ will indicate any of $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ or $\mathbb{Z}_p[x]$. Whereas $R[x]$ may indicate $\mathbb{Z}[x]$ or $\mathbb{Z}_n[x]$ for composite n as well.

Addition of polynomials is defined as follows:

$$\sum_{i=0}^{n} r_i x^i + \sum_{i=0}^{n} s_i x^i = \sum_{i=0}^{n} (r_i + s_i) x^i.$$

Multiplication is defined by the rule

$$(rx^m)(sx^n) = (rs)x^{m+n}$$

together with the consequences of the distributive law, i.e.

$$\Big(\sum_{i=0}^{m} r_i x^i\Big)\Big(\sum_{j=0}^{n} s_j x^j\Big) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} r_i s_j\Big) x^k.$$

The zero element is the constant zero polynomial $0 \in R \subset R[x]$, and the multiplicative identity is the constant polynomial $1 \in R \subset R[x]$. One checks that with these operations, $R[x]$ is a ring. If R is a commutative ring, then we see $R[x]$ is as well.

The **degree** of a non-zero polynomial $p(x) = \sum_{i=0}^{m} p_i x^i$ is the largest integer $\deg(p) = d$ so that $p_d \neq 0$. There is no natural degree for the 0 polynomial, but it is convenient to define $\deg(0) = -\infty$ since it makes the following lemma work.

6.1.1. Lemma. *Let R be an integral domain. Then $R[x]$ is an integral domain. Furthermore, if $p, q \in R[x]$, then*

$$\deg(pq) = \deg(p) + \deg(q).$$

Proof. If $p = 0$, then $pq = 0$ and we see

$$\deg(pq) = -\infty = -\infty + \deg(q) = \deg(p) + \deg(q).$$

Therefore, we may assume both p and q are non-zero. Let $\deg(p) = d$ and $\deg(q) = e$ with $d, e \geq 0$. Then

$$p(x) = p_d x^d + \text{ lower order terms } = \sum_{i=0}^{d} p_i x^i$$

$$q(x) = q_e x^e + \text{ lower order terms } = \sum_{j=0}^{e} q_j x^j$$

Thus a computation shows that

$$pq(x) = (p_d q_e) x^{d+e} + \text{ lower order terms.}$$

Since $p_d, q_e \neq 0$ and R is an integral domain, $p_d q_e \neq 0$. Therefore, $pq \neq 0$ and

$$\deg(pq) = d + e = \deg(p) + \deg(q),$$

as desired. ■

Observe that if R is not an integral domain, then Lemma 6.1.1 fails. For example, if $R = \mathbb{Z}_6[x]$, $p = 2x^3 + 1$ and $q = 3x$, then $pq = 3x$ so $\deg(pq) = 1 \neq 4 = \deg(p) + \deg(q)$.

Even when $\mathbb{F}$ is a field, the ring $\mathbb{F}[x]$ is not a field. The element x never has an inverse in $\mathbb{F}[x]$, as the following lemma shows.

6.1.2. Lemma. *If R is an integral domain, then the units*

$$R[x]^* = R^*.$$

In particular, for a field $\mathbb{F}$, the group of units $\mathbb{F}[x]^* = \mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

Proof. If $r \in R^*$, then there exists $s \in R^*$ such that $rs = 1$. This equality persists in $R[x]$, so $r \in R[x]^*$.

Conversely, if $p \in R[x]^*$, then there exists $q \in R[x]$ such that $pq = 1$. Applying Lemma 6.1.1, we have

$$0 = \deg(1) = \deg(p) + \deg(q).$$

Since p and q are non-zero, $\deg(p), \deg(q) \geq 0$. Thus, $\deg(p) = \deg(q) = 0$, i.e. $p, q \in R$, so $p \in R^*$. ■

Again, this may be false if R has zero divisors. For example, consider $\mathbb{Z}_4$.

$$(2x+1)^2 = 4x^2 + 4x + 1 \equiv 1 \pmod 4.$$

So $2x + 1$ is a unit of $\mathbb{Z}_4[x]$. Notice how the degree of the product turned out to be smaller than expected.

We end this section with two useful lemmas whose proofs we leave as exercises. Lemma 6.1.4 explains why the notation $\sum_{i=0}^{n} r_i x^i$ is particularly helpful: we can plug in elements of R in place of x.

6.1.3. Lemma. *Let $n \geq 2$ be an integer and let*

$$\pi \colon \mathbb{Z}[x] \to \mathbb{Z}_n[x]$$

be the function defined by

$$\pi\Big(\sum_{i=0}^{n} r_i x^i\Big) = \sum_{i=0}^{n} [r_i] x^i$$

where $[r]$ is the equivalence class of r in $\mathbb{Z}_n$. Then π is a ring homomorphism, i.e. $\pi(1) = 1$, $\pi(r+s) = \pi(r)+\pi(s)$, and $\pi(rs) = \pi(r)\pi(s)$ for all $r, s \in \mathbb{Z}[x]$.

6.1.4. Lemma. *Let R be a commutative ring and let $a \in R$. Consider the evaluation map*

$$\mathrm{ev}_a \colon R[x] \to R$$

defined by

$$\mathrm{ev}_a\Big(\sum_{i=0}^{n} r_i x^i\Big) = \sum_{i=0}^{n} r_i a^i.$$

Then ev_a is a ring homomorphism.

Exercises

1. Prove Lemma 6.1.3.

2. Prove Lemma 6.1.4.

3. Let $\mathbb{F}$ and $\mathbb{G}$ be fields with $\mathbb{F} \subset \mathbb{G}$. Prove that if $p, q \in \mathbb{F}[x]$, then $p \mid q$ in $\mathbb{F}[x]$ if and only if $p \mid q$ in $\mathbb{G}[x]$.

4. Show that Exercise 3 is false if $\mathbb{F}$ and $\mathbb{G}$ are allowed to be rings instead of fields.

5. Show that if R is an integral domain, then $R[x]$ is also an integral domain.

6. (Field generated by an element) Let $\mathbb{F}$ and $\mathbb{G}$ be fields with $\mathbb{F} \subset \mathbb{G}$. Let $\alpha \in \mathbb{G}$ and let

$$\mathbb{F}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in \mathbb{F}[x],\ g(\alpha) \neq 0 \right\}.$$

Prove that $\mathbb{F}(\alpha)$ is a field with $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{G}$. It is referred to as the *field generated by* α.

7. (Multivariate polynomial rings) Let R be a ring. Define $R[x_1, \ldots, x_n]$ to be the set of formal sums $\sum_{j=0}^{n} \sum_{i_j=0}^{d_j} r_{i_1,\ldots,i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ with coefficients $r_{i_1,\ldots,i_n} \in R$. Define addition and multiplication analogously to how it was defined for $R[x]$. Prove that $R[x_1, \ldots, x_n]$ is a ring.

8. Let R be a ring. Show $(R[x])[y]$, $(R[y])[x]$, and $R[x, y]$ are isomorphic.

6.2. Unique Factorization for Polynomials

In this section, we will prove the division algorithm for polynomials, and show, as for the integers, that this leads to a Euclidean algorithm and unique factorization in $\mathbb{F}[x]$, where $\mathbb{F}$ is a field.

6.2.1. Definition. If R is a commutative ring, a non-constant polynomial p in $R[x]$ is called **irreducible** if for every factorization $p = qr$ in $R[x]$, either $q(x)$ or $r(x)$ is a unit.

Notice that this definition is a special case of the one given in Definition 1.8.6. In particular, it coincides with the definition of a prime in $\mathbb{Z}$ or $\mathbb{Z}[\sqrt{d}]$. The term irreducible is used instead of prime for historical reasons. We are primarily interested in polynomials over a field. However, we will have reason to consider polynomials in $\mathbb{Z}[x]$.

The (long) division algorithm for polynomials is often taught high school. The technique is to divide the leading term of p into the leading term of q. Subtraction leaves a remainder of lower degree. Proceed iteratively until a remainder of degree less than $\deg(p)$ is achieved. This can easily be done by hand, or by computer.

6.2.2. Proposition (Division algorithm for polynomials). *Suppose that $q \neq 0$ and p belong to $\mathbb{F}[x]$. Then there is a unique quotient a and remainder r in $\mathbb{F}[x]$ so that*

$$p = aq + r \quad \textit{and} \quad \deg(r) < \deg(q).$$

Proof. Proceed by induction on the degree of p. If $d := \deg(p) < \deg(q)$, take $a = 0$ and $r = p$. Otherwise, $d \geq \deg(q) =: n$. Suppose that the result holds for all polynomials of degree less than d. Let

$$q = q_n x^n + \text{lower order terms} \quad \text{and} \quad p = p_d x^d + \text{lower order terms},$$

where q_n and p_d are non-zero. The polynomial

$$\begin{aligned} p_1(x) &= p(x) - (p_d q_n^{-1}) x^{d-n} q(x) \\ &= \big(p_d x^d + \text{lower order terms}\big) - \big(p_d x^d + \text{lower order terms}\big) \\ &= \text{lower order terms}. \end{aligned}$$

It follows that $\deg(p_1) < d = \deg(p)$. So by the induction hypothesis, the polynomial p_1 can be written as $p_1 = a_1 q + r$ where a_1 and r belong to $\mathbb{F}[x]$ and $\deg(r) < \deg(q)$. Therefore,

$$\begin{aligned} p(x) &= p_1(x) + (p_d q_n^{-1}) x^{d-n} q(x) \\ &= \big((p_d q_n^{-1}) x^{d-n} + a_1(x)\big) q(x) + r(x). \end{aligned}$$

This establishes existence.

For uniqueness, notice that if $q|p$ and $\deg(p) < \deg(q)$, then $p = 0$. This is because the identity $p = aq$ implies that

$$\deg(p) = \deg(a) + \deg(q).$$

Only $\deg(p) = \deg(a) = -\infty$ makes this possible, for otherwise the right-hand side is strictly larger. So $p = a = 0$.

Now suppose that $p = a_1 q + r_1 = a_2 q + r_2$ where both remainders have degree less than $\deg(q)$. Then q divides $(a_1 - a_2)q = r_2 - r_1$. Since

$$\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\} < \deg(q),$$

the previous argument shows that $r_2 - r_1 = 0$. Therefore we obtain $r_1 = r_2$ and $a_1 = a_2$. ■

6.2.3. Corollary. *The linear polynomial $x - c$ divides a polynomial p if and only if $p(c) = 0$.*

Proof. Divide $x - c$ into p by the division algorithm to obtain a quotient a and leave a remainder r of degree at most 0. So r is a constant. Then

$$p(c) = a(c)(c - c) + r = r.$$

So $x - c$ divides p if and only if the remainder $p(c)$ equals 0. ■

6.2.4 Euclidean algorithm for Polynomials. *If p and q are non-zero elements of $\mathbb{F}[x]$, then there exists a greatest common divisor d in $\mathbb{F}[x]$ with the properties:*

(1) *$d|p$ and $d|q$,*
(2) *there are polynomials s and t such that $d = ps + qt$,*
(3) *if $b|p$ and $b|q$, then $b|d$.*

Proof. By Proposition 6.2.2, $\mathbb{F}[x]$ is a Euclidean domain. So, the result follows from Theorem 1.8.12. ■

It follows that we obtain the important consequence of unique factorization for polynomials over a field.

6.2.5 Unique Factorization for Polynomials. *Every polynomial in $\mathbb{F}[x]$ factors uniquely into a product of irreducibles. That is, if $r(x)$ factors into irreducible terms as*

$$r = \prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j,$$

then $m = n$, and there is a permutation π and non-zero scalars $c_i \in \mathbb{F}^*$ so that $q_{\pi(i)} = c_i p_i$.

Proof. By Proposition 6.2.2 and Remark 1.8.9, the hypotheses of Theorem 1.8.18 hold. So, $\mathbb{F}[x]$ has unique factorization. ■

Exercises

1. Find $\gcd(f, g)$ and express it as a polynomial combination of f and g for the following examples in $\mathbb{Q}[x]$.
(a) $f(x) = x^4 + 7x^3 + 18x^2 + 20x + 8$ and
$g(x) = x^4 + 6x^3 + 7x^2 - 6x - 8$.
(b) $f(x) = 2x^4 + 3x^3 + 2x^2 + 3x + 2$ and $g(x) = x^4 + x^3 - x - 1$.

2. Factor $p(x) = x^4 + 1$ completely into irreducibles in each of the following:
(a) (i) $\mathbb{Q}[x]$ (ii) $\mathbb{R}[x]$ (iii) $\mathbb{C}[x]$.
(b) (i) $\mathbb{Z}_2[x]$ (ii) $\mathbb{Z}_5[x]$ (iii) $\mathbb{Z}_7[x]$.

3. (a) Show that a polynomial $p \in \mathbb{F}[x]$ of degree 2 or 3 is irreducible if and only if it has no roots in $\mathbb{F}$.
(b) Give an example that shows that this is false for degree 4.

4. Let $f \in \mathbb{Q}[x]$, and let f' be its derivative. Suppose that $p(x)$ is an irreducible polynomial. Show that $p|\ \gcd(f, f')$ if and only if $p^2|f$.

5. Show by example that Proposition 6.2.2 is false if $\mathbb{F}$ is replaced by an arbitrary commutative ring.

6. Let $\mathbb{F}$ and $\mathbb{G}$ be fields with $\mathbb{F} \subset \mathbb{G}$. Let $p, q \in \mathbb{F}[x]$. Let f be $\gcd(p, q)$ computed in $\mathbb{F}$ and let g be $\gcd(p, q)$ computed in $\mathbb{G}$. Prove that $f = g$.

6.3. Irreducible Polynomials in $\mathbb{Z}[x]$

Any polynomial in $\mathbb{Q}[x]$ can be multiplied by a large integer to clear the denominators and leave a polynomial with integer coefficients. It is a convenient fact, proven by Gauss, that a polynomial in $\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ only if it factors in $\mathbb{Z}[x]$. In other words, it is not necessary to use fractions to factor integer polynomials over the rationals. This makes it possible to obtain certain simple tests providing sufficient conditions for irreducibility.

6.3.1. Definition. A polynomial in $\mathbb{Z}[x]$ is called **primitive** if the gcd of its set of coefficients is equal to 1.

6.3.2. Lemma. *If r and s are primitive polynomials in $\mathbb{Z}[x]$, then rs is also primitive.*

Proof. Suppose the coefficients of rs have gcd not equal to 1. Then there exists a prime p that divides all of the coefficients of rs. Given a polynomial $f \in \mathbb{Z}[x]$, let $\pi(f) \in \mathbb{Z}_p[x]$ denote the polynomial obtained by reducing the coefficients mod p, as in Lemma 6.1.3. Then $\pi(r)\pi(s) = \pi(rs) = 0$. By Lemma 6.1.1, $\mathbb{Z}_p[x]$ is an integral domain, so either $\pi(r) = 0$ or $\pi(s) = 0$. Without loss of generality, $\pi(r) = 0$. In other words, p divides all of the coefficients of r, and therefore r is not primitive. ■

6.3.3 Gauss's Lemma. *A polynomial $p \in \mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ only if it factors in $\mathbb{Z}[x]$. Furthermore, if p factors as $p = rs$ in $\mathbb{Q}[x]$, then there are rational multiples r' of r and s' of s such that $r', s' \in \mathbb{Z}[x]$ and $p = r's'$.*

Proof. Suppose that p factors as $p = rs$ in $\mathbb{Q}[x]$. Choose integers M and N so that Mr and Ns have integer coefficients. Let m be the gcd of the coefficients of Mr, so that $Mr = mr_1$ where r_1 is a primitive polynomial in $\mathbb{Z}[x]$. Similarly, let n be the gcd of the coefficients of Ns, and factor $Ns = ns_1$ where s_1 is also primitive.

Compute

$$MNp = (Mr)(Ns) = mn(r_1 s_1). \tag{6.3.4}$$

By the lemma above, the polynomial $r_1 s_1$ is primitive. So the gcd of the coefficients of this product is mn. Let d be the gcd of the coefficients of p. We obtain the equation

$$MNd = mn.$$

Thus, dividing equation (6.3.4) by $MN = \frac{mn}{d}$ yields

$$p = dr_1 s_1,$$

which is a factorization in $\mathbb{Z}[x]$. Taking $r' = dr_1 = \frac{Md}{m} r$ and $s' = s_1 = \frac{N}{n} s$, we have completed the proof. ■

The following corollary of Gauss's Lemma characterizes irreducible polynomials in $\mathbb{Z}[x]$.

6.3.5. Corollary. *Let $p \in \mathbb{Z}[x]$. Then p is irreducible in $\mathbb{Z}[x]$ if and only if p is primitive and irreducible in $\mathbb{Q}[x]$.*

Proof. First suppose $p(x)$ is irreducible in $\mathbb{Z}[x]$. Gauss's Lemma 6.3.3 shows that $p(x)$ remains irreducible in $\mathbb{Q}[x]$. Now, let d be the greatest common divisor of the coefficients of $p(x)$. Then $p(x) = dq(x)$ with $q(x) \in \mathbb{Z}[x]$. By irreducibility of p, we must have $d = 1$ and so p is primitive.

Conversely, suppose $p(x)$ is reducible in $\mathbb{Z}[x]$. Then we may factor $p(x) = q(x)r(x)$ with $q(x), r(x)$ non-zero non-units in $\mathbb{Z}[x]$. If both q and r have positive degree, then we see $p(x)$ is reducible in $\mathbb{Q}[x]$. If on the other hand, $\deg(q) = 0$, then $q \in \mathbb{Z}$ is a common factor of the coefficients of $p(x)$. Since q is not a unit in $\mathbb{Z}[x]$, we have $q \neq \pm 1$, showing $p(x)$ is not primitive. ■

The next result is a well known criterion for finding rational roots of polynomials in $\mathbb{Z}[x]$.

6.3.6 Rational Root Theorem. *If $\gcd(a, b) = 1$, and $\frac{a}{b}$ is a root of $p(x) = \sum_{i=0}^{m} p_i x^i \in \mathbb{Z}[x]$, then $b|p_m$ and $a|p_0$.*

Proof. By Corollary 6.2.3, $x - \frac{a}{b}$ is a factor of p in $\mathbb{Q}[x]$. The rational multiple of $x - \frac{a}{b}$ which is primitive is precisely $bx - a$. From Gauss's Lemma, $bx - a$ must be a factor of p. That is,

$$p(x) = (bx - a)q(x) = bq_{m-1}x^m + \ldots - aq_0.$$

So $p_m = bq_{m-1}$ and $p_0 = -aq_0$. ■

For example, consider the polynomial $x^3 + x + 1$. By the criterion above, the only possible rational roots are ± 1. Substituting ± 1 into the above polynomial, we see neither is a root. So this cubic has no linear factors. Therefore, it is irreducible.

Similarly, consider $p = x^4 + 2x^3 + 4x^2 + 4x + 4$. By the corollary, the only possibilities for rational roots are ± 1, ± 2, and ± 4. Trial shows that none are roots. (Clearly, p has no positive roots. This cuts down on the number of trials.) However, this only means that p has no *linear* factors. It does not imply that p is irreducible. And, in fact, it is not. It factors as

$$\begin{aligned} p(x) &= \left(x^2 + x + 2\right)^2 - x^2 \\ &= \left(x^2 + 2\right)\left(x^2 + 2x + 2\right) \end{aligned}$$

Exercises

1. Factor $8x^3 - 6x + 1$ in $\mathbb{Z}[x]$ or prove that it is irreducible.

2. Factor $x^4 - 5x^2 + 6x + 1$ in $\mathbb{Z}[x]$ or prove that it is irreducible.

3. Let $f(x) = x^5 + 3x^4 + 2x^3 + x^2 + x - 2$ and $g(x) = x^5 + 2x^4 + 2x^3 - x^2 - 4x + 2$.
(a) Find $\gcd(f, g)$.
(b) Hence factor f and g completely in $\mathbb{Z}[x]$.

4. Find a quartic polynomial in $\mathbb{Z}[x]$ with $\sqrt{5} - 2\sqrt{3}$ as a root. Factor it completely in $\mathbb{R}[x]$. Then prove that it is irreducible in $\mathbb{Q}[x]$.

5. Prove the following generalization of Gauss's Lemma 6.3.3. Let R be any UFD and let K be its fraction field, as defined in Exercise 5 of Section 2.4. Prove that a polynomial $p \in R[x]$ factors in $K[x]$ only if it factors in $R[x]$. Furthermore, prove that if p factors as $p = rs$ in $K[x]$, then there exist $a, b \in K^*$ such that $r' = ar \in R[x]$, $s' = bs \in R[x]$, and $p = r's'$.

6. (a) Prove that $\mathbb{Z}[x]$ is a UFD.
HINT: Use that $\mathbb{Q}[x]$ is a UFD.
(b)★ **(Gauss's Theorem on UFDs)** Prove that if R is a UFD, then $R[x]$ is a UFD.

6.4. Eisenstein's Criterion

In this section, we develop another test for irreducibility that carries these ideas a little further.

6.4.1 Eisenstein's Criterion. *Let $p = \sum_{k=0}^{d} p_k x^k \in \mathbb{Z}[x]$. Suppose that q is a prime integer such that $q \mid p_i$ for $0 \leq i < d$, q does not divide p_d, and q^2 does not divide p_0. Then p is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose to the contrary that p is reducible in $\mathbb{Q}[x]$. Then by Gauss's Lemma, we may write $p = rs$ in $\mathbb{Z}[x]$ with $\deg(r), \deg(s) > 0$. Write $r(x) = \sum_{i=0}^{I} r_i x^i$ and $s(x) = \sum_{j=0}^{J} s_j x^j$ with $r_I, s_J \neq 0$ and $I, J \geq 1$ Then $I, J < d$. The hypothesis tells us that q does not divide $p_d = r_I s_J$, hence q does not divide r_I and does not divide s_J. Since q does divide $p_0 = r_0 s_0$ but q^2 does not, it follows that q divides one of r_0 or s_0, but not the other. Without loss of generality, $q | r_0$ and q does not divide s_0. Let $i_0 \leq I$ be the least integer for which q does not divide r_{i_0}. Then

$$p_{i_0} = (r_0 s_{i_0} + \ldots + r_{i_0 - 1} s_1) + r_{i_0} s_0.$$

From the choice of i_0, it follows that q divides each term in the bracketed sum, but does not divide $r_{i_0}s_0$. Thus q does not divide p_{i_0}. Since $i_0 \leq I < d$, this is contrary to the hypotheses. Therefore p must be irreducible. ■

6.4.2. Example. For example, let us find an irreducible polynomial with $\sin(\frac{2\pi}{7})$ as a root using de Moivre's Theorem. Let us write $c := \cos(\frac{2\pi}{7})$ and $s = \sin(\frac{2\pi}{7})$. Using the formula

$$1 = \cos(2\pi) + i\sin(2\pi) = (c + is)^7,$$

and taking the imaginary part of both sides, one obtains

$$\begin{aligned} 0 &= 7c^6s - 35c^4s^3 + 21c^2s^5 - s^7 \\ &= 7(1-s^2)^3s - 35(1-s^2)^2s^3 + 21(1-s^2)s^5 - s^7 \\ &= -s(64s^6 - 112s^4 + 56s^2 - 7) \end{aligned}$$

Since $s = \sin(\frac{2\pi}{7}) \neq 0$, it is a root of the polynomial

$$p(x) = 64x^6 - 112x^4 + 56x^2 - 7.$$

This polynomial is a perfect candidate for Eisenstein's criterion. Note that $\gcd(64, 7) = 1$, but 7 divides -112, 56 and -7. Since 7^2 does not divide -7, it follows that p is irreducible in $\mathbb{Z}[x]$ and hence in $\mathbb{Q}[x]$. In particular, p has no rational roots. So $\sin(\frac{2\pi}{7})$ is irrational.

6.4.3. Example. Sometimes, one has to be clever to find a way to use Eisenstein's criterion. Let q be an integer prime. Let

$$p(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \ldots + x + 1.$$

There is no obvious way to use the method here. However, sometimes a substitution helps. Notice that $p(x)$ factors as $p = rs$ if and only if $p(x+1)$ factors as $p(x+1) = r(x+1)s(x+1)$. So compute

$$\begin{aligned} p(x+1) &= \frac{(x+1)^q - 1}{(x+1) - 1} \\ &= x^{-1}\sum_{k=1}^{q}\binom{q}{k}x^k = \sum_{k=1}^{q}\binom{q}{k}x^{k-1} \\ &= x^{q-1} + qx^{q-2} + \frac{q(q-1)}{2}x^{q-3} + \ldots + \frac{q(q-1)}{2}x + q \end{aligned}$$

Notice that the leading coefficient is $\binom{q}{q} = 1$, the constant coefficient is $\binom{q}{1} = q$, and the other coefficients are $\binom{q}{k} = \frac{q!}{k!(q-k)!}$ for $2 \leq k \leq q-1$. This is always an integer. Now q divides the numerator, but not the denominator. Thus each is divisible by q, while the constant coefficient is not divisible by

q^2. So $p(x+1)$ satisfies Eisenstein's criterion, and thus is irreducible. So p is irreducible as well.

The roots of p are the $q-1$ q-th roots of unity other than 1, namely $e^{2k\pi i/q}$ for $1 \le k \le q-1$.

Exercises

1. Prove that $x^5 - 210x^4 - 903x^3 + 168x - 315$ is irreducible in $\mathbb{Z}[x]$.

2. If $n > 1$ is a square free integer, show that $x^d - n$ is irreducible in $\mathbb{Z}[x]$.

3. Prove that $x^5 - 22x^4 + 196x^3 - 887x^2 + 2036x - 1886$ is irreducible in $\mathbb{Z}[x]$.
HINT: substitute $x - 1$ for x.

4. Prove that $x^7 - 14x^6 + 84x^5 - 280x^4 + 560x^3 - 672x^2 + 459x - 29$ is irreducible in $\mathbb{Z}[x]$.
HINT: find a substitution that helps.

5. Prove that if n is composite, the polynomial $x^{n-1} + x^{n-2} + \cdots + x + 1$ is reducible.

6. (**Schur**) Prove the following special case of a result of Schur: if p is prime and $a_1, \ldots, a_{p-1} \in \mathbb{Z}$, the polynomial $1 + \sum_{k=1}^{p-1} \frac{a_k}{k!} x^k + \frac{x^p}{p!}$ is irreducible in $\mathbb{Q}[x]$.

7. Prove the following generalization of Eisenstein's Criterion 6.4.1. Let R be any UFD and let K be its fraction field, as defined in Exercise 5 of Section 2.4. Let $q \in R$ be irreducible and let $p = \sum_{k=0}^{d} p_k x^k \in R[x]$. Suppose that $q \mid p_i$ for $0 \le i < d$, q does not divide p_d, and q^2 does not divide p_0. Prove p is irreducible in $K[x]$.

8. Prove $x^n + y^n - 1$ is irreducible in $\mathbb{Q}[x, y]$ for all $n \ge 1$.
HINT: consider this as an element of $(\mathbb{Q}[x])[y]$ and note that $x^n - 1$ has a linear factor.

6.5. Factoring Modulo Primes

Another simple test for irreducibility is to study the factorization of $f(x)$ modulo p for various small primes p.

6.5.1. Lemma. *If $f \in \mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$, then it is reducible modulo p for every prime p relatively prime to the leading coefficient of f.*

The reason for the condition on p in Lemma 6.5.1 is so that the degree of f does not decrease when moving to $\mathbb{Z}_p$. For example, the reducible

polynomial $f(x) = 2x^2 + 3x + 1 = (2x + 1)(x + 1)$ reduces to $f \equiv x + 1 \pmod 2$ which is irreducible.

Proof of Lemma 6.5.1. Fix a prime p. For any $h \in \mathbb{Z}[x]$, let $\pi(h) \in \mathbb{Z}_p[x]$ be as in Lemma 6.1.3. By Gauss's Lemma, we may write $f = rs$ in $\mathbb{Z}[x]$ with $\deg(r), \deg(s) > 0$. Then $\pi(f) = \pi(r)\pi(s)$. The product of the leading coefficients of r and s is the leading coefficient of f, and hence the leading coefficients of r and s are relatively prime to p. So

$$\deg(\pi(r)) = \deg(r) \quad \text{and} \quad \deg(\pi(s)) = \deg(s).$$

Hence both $\pi(r)$ and $\pi(s)$ are non-trivial factors in $\mathbb{Z}_p[x]$. ■

We state the contrapositive form as a corollary.

6.5.2. Corollary. *If $f \in \mathbb{Z}[x]$ has leading coefficient coprime to p, and f is irreducible modulo p, then f is irreducible in $\mathbb{Q}[x]$.*

6.5.3. Example. Let $f(x) = x^5 + 5x^4 + 6x + 1$. By Gauss's Lemma, the only possible roots are ± 1, neither of which works. So, if f factors at all, it must be into a product of a cubic and a quadratic polynomial. Modulo 3, this polynomial is

$$f(x) \equiv x^5 - x^4 + 1 \pmod 3.$$

The simplest approach is to find all the irreducible quadratic polynomials in $\mathbb{Z}_3[x]$, and test them. The reducible quadratics are the ones with zero constant coefficient, and the three products $(x \pm 1)(x \pm 1)$; namely, x^2, $x^2 \pm x$, $x^2 - 1$, and $x^2 \pm x + 1$. That leaves $x^2 + 1$ and $x^2 \pm x - 1$ as the three irreducible monic quadratic polynomials in $\mathbb{Z}_3[x]$. A calculation shows that none of them divide $f(x)$. Hence f is irreducible in $\mathbb{Z}_3[x]$. Therefore it is irreducible over the rationals as well.

6.5.4. Example. This method can also be used to factor polynomials, by using the Chinese Remainder Theorem. Consider $f(x) = x^5 - 12x^3 + 17x^2 - 10x + 2$. The only possible rational roots are ± 1 and ± 2, none of which work. So if this factors, it is into the product of a cubic and a quadratic. Suppose that we have factored it mod 3 and mod 5 into irreducible factors.

$$f(x) \equiv (x^3 - x - 1)(x^2 + 1) \pmod 3$$
$$f(x) \equiv (x^3 + 3x^2 + x + 2)(x + 1)^2 \pmod 5$$

The cubic term $g(x)$, if it exists, is congruent to $x^3 - x - 1 \pmod 3$ and congruent to $x^3 + 3x^2 + x + 2 \pmod 5$. Solving this system of equations, we find that

$$g(x) \equiv x^3 + 3x^2 + 11x + 2 \pmod{15}.$$

Moreover, the leading coefficient divides 1, and hence must be 1; and the constant coefficient must divide 2. So it must be 2. Let us write $g(x) = x^3 + ax^2 + bx + 2$.

This forces the constant coefficient of the quadratic term $h(x)$ to be 1. Since the coefficient of x^4 in $f(x)$ is 0, the coefficient of x in h must be $-a$. Let's write $h(x) = x^2 - ax + 1$. Trial of small choices for a and b now yields the factorization

$$x^5 - 12x^3 + 17x^2 - 10x + 2 = (x^3 + 3x^2 - 4x + 2)(x^2 - 3x + 1).$$

This kind of search can be carried out with reasonable efficiency on a computer. However, this is not the standard algorithm used on computers to factor polynomials. The methods used will be discussed at the end of the next chapter.

Exercises

1. Reduce the polynomial in Section 6.43 modulo 3 and factor it completely. Use this to show that the polynomial is irreducible in $\mathbb{Z}[x]$.

2. Reduce the polynomial in Section 6.44 modulo 2. Use this to show that the polynomial is irreducible in $\mathbb{Z}[x]$.

3. Decide if $x^5 + 2x + 4$ is irreducible in $\mathbb{Z}[x]$ by reducing mod 3.

4. Prove that $p(x) = x^4 + 1$ is reducible in $\mathbb{Z}_p[x]$ for every prime p. (Compare with Section 6.2 2.)
HINT: you need to know when $-1, \pm 2$ are squares mod p.

5. The polynomial $q(x) = x^6 - 6x^4 + 14x^3 + 12x^2 + 84x + 41$ factors as

$$q \equiv (x^2 - x - 1)^3 \pmod 3 \quad \text{and} \quad q \equiv (x-3)^3(x+3)^3 \pmod 7.$$

Show that q is irreducible.

6. Show that if n is odd and p is prime, then $f(x) = x^n - p^2$ is irreducible in $\mathbb{Z}[x]$.
HINT: if $f = gh$, then $g(x^2)h(x^2) = (x^n - p)(x^n + p)$.

7. Show that $x^4 + 12x^2 + 18x + 6$ is irreducible in $(\mathbb{Z}[i])[x]$. Remember that 2 is not a prime in the Gaussian integers.

8. **(Perron's irreducibility criterion)**
Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbb{Z}$ and suppose

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Prove that f is irreducible in $\mathbb{Z}[x]$.
HINT: Use Section 5.5, Exercise 5.

9. **(A variant on Cohn's irreducibility criterion)**
Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_i \in \mathbb{Z}$ and $a_d \neq 0$. Suppose

there is $n \in \mathbb{Z}$ with $f(n)$ prime and

$$n \geq 2 + \max_{0 \leq i < d} \left| \frac{a_i}{a_d} \right|.$$

Prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$.[1]
HINT: Use Section 5.5, Exercise 2 to bound the roots of f. Show that if $f = gh$, then $|g(n)| > 1$.

6.6. Algebraic Numbers

6.6.1. Definition. A complex number w is called **algebraic** if it is the root of a polynomial in $\mathbb{Q}[x]$. A monic polynomial p in $\mathbb{Q}[x]$ of least degree such that $p(w) = 0$ is called the **minimal polynomial** of w.

We will establish that the minimal polynomial is unique. No particular properties of the field of rational numbers is used here. Indeed, if $\mathbb{F}$ is any field contained in a larger field $\mathbb{G}$ and $w \in \mathbb{G}$ is a root of a polynomial in $\mathbb{F}[x]$, then the minimal polynomial of w is the monic polynomial of least degree in $\mathbb{F}[x]$ with w as a root. The following result is valid in this greater generality without any change in the proof.

6.6.2. Theorem. *The minimal polynomial p of an algebraic number w is unique. Moreover, p is irreducible, and if q is another polynomial such that $q(w) = 0$, then p divides q.*

Proof. If q and r are two polynomials such that $q(w) = r(w) = 0$, let $s = \gcd(q, r)$. By the Euclidean algorithm for $\mathbb{Q}[x]$, there are polynomials a and b in $\mathbb{Q}[x]$ so that $s = aq + br$. Hence

$$s(w) = a(w)q(w) + b(w)r(w) = 0.$$

In particular, the monic polynomial $t = \gcd(p, q)$ satisfies $t(w) = 0$. Thus $\deg(t) \geq \deg(p)$. Since $t|p$, it follows that t and p are scalar multiples of one another. Since p and t are monic, it follows that $t = p$. Hence, p also divides q.

Suppose that p is not irreducible over $\mathbb{Q}[x]$, say $p = qr$ where q and r are non-constant polynomials in $\mathbb{Q}[x]$. But then

$$0 = p(w) = q(w)r(w).$$

So either $q(w) = 0$ or $r(w) = 0$. But this is impossible, as they have smaller degree than p, which is the polynomial of smallest degree in $\mathbb{Q}[x]$ with w as a root. Hence p must be irreducible. ■

This immediately yields a powerful test for irrationality of algebraic numbers.

[1] This variant of Cohn's irreducibility criterion is due to Murty [**27**].

6.6.3. Corollary. *If w is a root of an irreducible polynomial p in $\mathbb{Z}[x]$ of degree at least 2, then w is irrational.*

Proof. From the hypothesis, it follows that p is the minimal polynomial of w (up to a scalar). The minimal polynomial of a rational number r is $x - r$, which has degree 1. So w is irrational. ■

6.6.4. Example. If $|n| > 1$ is square free, the polynomial $x^k - n$ is irreducible by Eisenstein's criterion. Just take any prime p dividing n, and note that p divides all the zero coefficients, and p^2 does not divide n. So $x^k - n$ is the minimal polynomial of $\sqrt[k]{n}$. This gives another proof of the irrationality of $\sqrt[k]{n}$.

6.6.5. Example. Let $w = \sqrt[3]{3} - \sqrt{2}$. Notice that

$$3 = (w + \sqrt{2})^3 = w^3 + 3\sqrt{2}w^2 + 6w + 2\sqrt{2}.$$

Hence we may compute

$$\begin{aligned}(w^3 + 6w - 3)^2 &= (3\sqrt{2}w^2 + 2\sqrt{2})^2\\ w^6 + 12w^4 - 6w^3 + 36w^2 - 36w + 9 &= 18w^4 + 24w^2 + 8\\ w^6 - 6w^4 - 6w^3 + 12w^2 - 36w + 1 &= 0.\end{aligned}$$

From the rational roots theorem, the only possible rational roots of the polynomial $p(x) = x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1$ are ± 1, neither of which works.

In fact, p is irreducible in $\mathbb{Q}[x]$. By Gauss's Lemma, it suffices to show that p is irreducible in $\mathbb{Z}[x]$. To see this, reduce it mod 3. The polynomial factors as

$$p \equiv (x^2 + 1)^3 \pmod 3$$

and $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$ since it has no roots in $\mathbb{Z}_3$. So if p factors in $\mathbb{Z}[x]$, it factors as a quadratic times a quartic. The quadratic must be $x^2 + 3ax + 1$. There are two ways to proceed, and both are computational. One is to write down a general quartic, multiply it by $x^2 + 3ax + 1$, and set it equal to p. Then a calculation shows that the equations can't be solved. Since the coefficients of x and x^3 are forced, simple conditions on a and the coefficient b of x^2 lead to a contradiction. Alternatively, we can factor p mod 7 as

$$p(x) \equiv (x^3 - 2x^2 - x - 2)(x^3 + 2x^2 - x + 3) \pmod 7.$$

You can check quickly that neither cubic has a root in $\mathbb{Z}_7$, and thus they are irreducible. This shows that any factorization in $\mathbb{Z}[x]$ must be into cubics. This is incompatible with the factorization mod 3. So p is irreducible.

It is a non-trivial fact that if u and v are algebraic numbers, then $u+v$, uv and (when $v \neq 0$) u/v are all algebraic numbers. This will be proven in Theorem 6.9.3.

Exercises

1. Show that $\sin(1^\circ) = \sin(\frac{\pi}{180})$ is algebraic.

2. (a) Find a polynomial p in $\mathbb{Z}[x]$ with $\sqrt{3} + \sqrt[3]{5}$ as a root.
(b) Hence prove that $\sqrt{3} + \sqrt[3]{5}$ is irrational.
(c) Suppose you have calculated that p factors modulo 3 as $(x+1)^6$, and modulo 5 as $(x^2+2)^3$. Show that p is irreducible.

3. Find the minimal polynomial of $\sqrt{2} - \sqrt[3]{7}$.

4. Let $\mathbb{F}$ be a field and let $p(x) = a_0 + a_1x + \ldots + a_nx^n$ and $q(x) = a_n + a_{n-1}x + \ldots + a_0x^n$ belong to $\mathbb{F}[x]$. If $a_0a_n \neq 0$, what is the relationship between the roots of p and the roots of q? Hence conclude that if α is algebraic over $\mathbb{F}$, then so is $1/\alpha$.

5. **(Primitive Element Theorem)** Let α and β be algebraic numbers. Recall the definition of a field generated by an element given in Exercise 6 of Section 6.1. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α and let $g(x) \in \mathbb{Q}[x]$ be the minimal polynomial of β.
(a) Prove there exists $c \in \mathbb{Q}$ such that β is the only common complex root of $g(x)$ and $h(x) = f(\alpha + c(\beta - x))$.
(b) Let $\gamma = \alpha + c\beta$. Prove that $\gcd(g,h) = w(x-\beta) \in \mathbb{Q}(\gamma)$.
HINT: Use Exercise 6 from Section 6.2.
(c) Prove that $\alpha, \beta \in \mathbb{Q}(\gamma)$ and conclude that $\mathbb{Q}(\alpha)(\beta) = \mathbb{Q}(\gamma)$.
(d) Prove that if $\alpha_1, \ldots, \alpha_n$ are algebraic numbers, then there exists δ such that $\mathbb{Q}(\alpha_1)(\alpha_2)\cdots(\alpha_n) = \mathbb{Q}(\delta)$.

6.7. Transcendental Numbers

A complex number which is not algebraic is called **transcendental**. In this section, we will establish that various complex numbers are transcendental. This problem has a long history. Liouville showed that certain numbers were transcendental in 1851. However, his methods did not apply to many naturally occurring numbers, such as π and e. In 1873, Hermite showed that e was transcendental. And in 1882, Lindemann generalized his argument to show that any non-trivial sum

$$\sum_{i=1}^{n} \alpha_i e^{\beta_i}$$

is never 0 if the $\alpha_i \neq 0$ are algebraic, and the β_i are distinct algebraic numbers. This means that π is not algebraic because

$$e^0 + e^{i\pi} = 0.$$

As 0, 1, and i are all algebraic, π must be transcendental. In 1934, Gelfond and Schneider proved that α^β is always transcendental if $\alpha \neq 0$ or 1 is algebraic, and β is an irrational algebraic number. In general, these results are very difficult. We will take a look at the results of Liouville and Hermite.

Liouville's result is based on the fact that irrational algebraic numbers cannot be approximated too quickly by rational numbers. This is made precise in the following theorem.

6.7.1. Theorem. *Suppose that w is a real root of an irreducible polynomial*

$$p(x) = \sum_{i=0}^{d} p_i x^i$$

in $\mathbb{Q}[x]$ of degree $d > 1$. Then there is a positive number $\delta > 0$ so that for every rational number $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ relatively prime, we have

$$\left| w - \frac{a}{b} \right| \geq \frac{\delta}{b^d}.$$

Proof. We will assume that p has integer coefficients, because this can easily be achieved by multiplying p by a large integer. Let

$$M = \max_{|x-w|\leq 1} |p'(x)| \leq \sum_{i=1}^{d} i|p_i|(|w|+1)^{i-1} < \infty.$$

The next observation is the key idea. The number $b^d p(\frac{a}{b})$ is a non-zero integer. It is an integer because

$$b^d p\big(\frac{a}{b}\big) = \sum_{i=0}^{d} p_i a^i b^{d-i}.$$

Since p is irreducible, it has no rational roots. Thus $b^d p(\frac{a}{b}) \neq 0$. A non-zero integer has modulus at least 1. Hence

$$\left| p\big(\frac{a}{b}\big) \right| \geq |b|^{-d}.$$

Now apply the mean value theorem. Suppose that $\left|\frac{a}{b} - w\right| \leq 1$. Then there is a real number c between w and $\frac{a}{b}$ so that

$$p\big(\frac{a}{b}\big) = p\big(\frac{a}{b}\big) - p(w) = p'(c)\big(w - \frac{a}{b}\big).$$

Hence

$$\left| w - \frac{a}{b} \right| = \frac{|p(\frac{a}{b})|}{|p'(c)|} \geq \frac{1}{M|b|^d}.$$

If we set $\delta = \min\{1, M^{-1}\}$, the desired formula holds. The hard part was done in the previous paragraph for fractions close to w. The remaining case, when $\left|w - \frac{a}{b}\right| > 1$, follows since $1 \geq \delta/|b|^d$. ■

6.7.2. Example. (**Liouville numbers**) Let $q > 1$ be an integer, and define

$$w = \sum_{k \geq 1} q^{-k!}.$$

Then w is transcendental. To see this, first observe that the base-q expansion of w is given by a sequence of 1's and 0's with a 1 in the $k!$-th decimal place; since this is a non-repeating sequence, w must be irrational. To prove w is transcendental, we may therefore apply Theorem 6.7.1. Let $b_n = q^{n!}$ and

$$a_n = q^{n!} \sum_{k=1}^{n} q^{-k!} = \sum_{k=1}^{n} q^{n!-k!}.$$

Notice that

$$\left|w - \frac{a_n}{b_n}\right| = \left| \sum_{k \geq n+1} q^{-k!} \right| < q^{-(n+1)!} \sum_{j \geq 0} q^{-j} < 2q^{-(n+1)!}$$

Consider any positive integer d. Then for all $n \geq d$,

$$b_n^d \left|w - \frac{a_n}{b_n}\right| < 2q^{-n!(n+1-d)} \leq 2q^{-n!}.$$

Since this tends to 0 as n tends to infinity, there is no integer d and positive δ such that

$$\left|w - \frac{a}{b}\right| \geq \frac{\delta}{b^d}$$

for all fractions. By Theorem 6.7.1, w cannot be algebraic.

For example, $w = \sum_{n \geq 1} 10^{-n!} = 0.11000100000000000000000010\ldots$ is transcendental.

Now let us consider the much more difficult task of showing that e is transcendental. This proof has been simplified over the years, but perhaps it will seem rather mysterious because so much of the 'scaffolding' has been removed in order to make it short. The proof uses calculus, not surprisingly, since it is in calculus that properties of e are developed. In particular, we use the fact that $\frac{d}{dx}(e^x) = e^x$.

6.7.3. Theorem. *e is transcendental.*

Proof. Suppose, to the contrary, that there are integers $a_0, \ldots, a_n$ so that

$$a_0 + a_1 e + a_2 e^2 + \ldots a_n e^n = 0.$$

We may assume that $a_n a_0 \neq 0$. For any large prime $p \gg \max\{|a_0|, n\}$, consider the polynomial

$$f(x) = \frac{1}{(p-1)!}x^{p-1}(1-x)^p(2-x)^p \dots (n-x)^p$$
$$= \frac{(n!)^p}{(p-1)!}x^{p-1} + \text{higher order terms} = \frac{1}{(p-1)!}\sum_{k=p-1}^{K} f_k x^k$$

where $K = (n+1)p - 1$ is the degree of f. Notice that the coefficients f_k are integers.

We need information about the values $f^{(j)}(i)$ for integers $j \geq 0$ and $0 \leq i \leq n$, where $f^{(j)}$ means the j-th derivative of f. Notice that for $j \geq p$,

$$f^{(j)}(x) = \sum_{k=j}^{K} \frac{k(k-1)(k-2)\dots(k+1-j)}{(p-1)!} f_k x^{k-j}$$
$$= \sum_{k=j}^{K} \binom{k}{j} j(j-1)\dots(p) f_k x^{k-j}$$

This polynomial has integer coefficients which are multiples of p. Hence

$$f^{(j)}(i) \equiv 0 \pmod{p} \quad \text{for} \quad j \geq p,\ i \in \mathbb{Z}.$$

Now f has a zero of order p at each integer $1 \leq i \leq n$. So each i is also a root of $f^{(j)}$ for $0 \leq j \leq p-1$. (See the exercises.) Hence

$$f^{(j)}(i) = 0 \quad \text{for} \quad 0 \leq j \leq p-1,\ 1 \leq i \leq n.$$

Similarly, since f has a zero of order $p-1$ at 0,

$$f^{(j)}(0) = 0 \quad \text{for} \quad 0 \leq j \leq p-2.$$

Finally, there is one term which is not a multiple of p,

$$f^{(p-1)}(0) = (n!)^p \not\equiv 0 \pmod{p}.$$

The next trick is to introduce the polynomial

$$F(x) = \sum_{j=0}^{K} f^{(j)}.$$

From the previous paragraph, we see that

$$F(i) \equiv 0 \pmod{p} \quad \text{for} \quad 1 \leq i \leq n$$

and

$$a_0 F(0) \equiv a_0 (n!)^p \not\equiv 0 \pmod{p}.$$

Since $a_0 = -a_1 e - a_2 e^2 - \ldots - a_n e^n$,

$$0 \not\equiv \sum_{i=0}^{n} a_i F(i) = \sum_{i=1}^{n} a_i (F(i) - e^i F(0))$$
$$= \sum_{i=1}^{n} a_i e^i \big(e^{-i} F(i) - e^0 F(0)\big) \pmod{p}.$$

Now it remains to estimate the size of this non-zero integer. Since $\deg(f) = K$, we have $f^{(K+1)} = 0$. A routine calculation shows that

$$\frac{d}{dt}\big(e^{-x} F(x)\big) = -e^{-x} \sum_{j=0}^{K} f^{(j)} + e^{-x} \sum_{j=0}^{K} f^{(j+1)} = -e^{-x} f(x)$$

By the mean value theorem, there are real numbers $c_i \in (0, i)$ so that

$$|e^{-i} F(i) - e^0 F(0)| = i \left| \frac{d}{dt} \left(e^{-x} F(x)\right)(c_i) \right| = i e^{-c_i} |f(c_i)|$$
$$\leq n \max_{0 \leq x \leq n} |f(x)| \leq \frac{n^{K+1}}{(p-1)!}$$

The last estimate comes from $(p-1)!|f(x)| = x^{p-1}(1-x)^p \cdots (n-x)^p \leq n^K$. Let $A = \max_{0 \leq j \leq n} |a_j|$. Then one can estimate

$$\Big| \sum_{i=1}^{n} a_i e^i \big(e^{-i} F(i) - e^0 F(0)\big) \Big| \leq \sum_{i=1}^{n} A e^n \frac{n^{K+1}}{(p-1)!}$$
$$= \frac{A e^n n^{K+2}}{(p-1)!} = \frac{A n e^n (n^{n+1})^p}{(p-1)!}.$$

So the idea is to choose a prime p so large that this fraction is less than 1. If this fraction is denoted as B_p, we see that for $p > 2n^{n+1}$,

$$\frac{B_{p+1}}{B_p} = \frac{n^{n+1}}{p} < \frac{1}{2}.$$

Thus, by the ratio test,

$$\lim_{p \to \infty} B_p = 0.$$

Choose the prime p so large that $B_p < 1$. However the left-hand side represents a non-zero integer. Clearly, this is contradictory.

Therefore e does not satisfy any algebraic equation over $\mathbb{Q}$. ■

Exercises

1. Show that $\sum_{n \geq 1} 2^{-n^n}$ is transcendental.

2. (a) Prove that if α is transcendental and $q \in \mathbb{Q} \setminus \{0, 1\}$, then α^q is transcendental.

(b) Give an example of a transcendental number α and an irrational number q such that α^q is algebraic.

3. (a) Show that if $p(x) = (x-a)^d q(x)$ is a polynomial in $\mathbb{R}[x]$, then $f^{(j)}$ has the form $(x-a)^{d-j} r(x)$ for all $j \leq d$.
(b) Moreover, if $q(a) \neq 0$, show that $r(a) \neq 0$.
(c) Show that a root a of $p(x)$ is simple if and only if $\gcd(p, p')(a) \neq 0$.

4. Show that if α is transcendental and $\beta \neq 0$ is algebraic, then $\alpha + \beta$, $\alpha\beta$ and α^{-1} are all transcendental.

5. If $0 \leq a_k \leq 9$ are integers for $k \geq 1$ and infinitely many are non-zero, then $w = \sum_{k \geq 1} a_n 10^{-k!}$ is transcendental.

6. (a) Show that if $\gcd(a, b) = 1$, then $\left|\sqrt{15} - \frac{a}{b}\right| > \frac{1}{9b^2}$.
(b) If n is a positive square free integer, find a C so that $\left|\sqrt{n} - \frac{a}{b}\right| > \frac{1}{Cb^2}$.

6.8. Sturm's Algorithm

Recall the factorization theorem 5.6.2 for real polynomials. Define the **discriminant** of a quadratic polynomial $p(x) = ax^2+bx+c$ by $\Delta(p) = b^2-4ac$. This theorem can be restated as:

6.8.1. Theorem. *The irreducible polynomials in $\mathbb{R}[x]$ are the linear polynomials, and the quadratic polynomials with negative discriminant. The roots of irreducible quadratic polynomials are a conjugate pair $\{a, \overline{a}\}$ of non-real complex numbers.*

As in Exercise 6.7 3 or Lemma 7.8.6, we may test for multiple roots by computing $\gcd(p, p')$. Moreover, all the roots are simple roots exactly when $\gcd(p, p') = 1$. (That lemma may be read independently of the rest of Chapter 7. It is easier in the case of the reals, and other fields of characteristic 0, because the derivative of a non-constant polynomial must be non-zero.)

We now describe an algorithm known as **Sturm's Algorithm** for counting the number of real roots of a real polynomial with simple roots in any interval. The key is the Euclidean algorithm with a special sign convention.

Start with a real polynomial $p(x)$ with simple roots. Set $p_0 = p$ and $p_1 = p'$. Apply the Euclidean algorithm by repeated use of the division algorithm. Recall that dividing p_i into p_{i-1} yields a quotient a_i and a remainder which we call $-p_{i+1}$, so that

$$p_{i-1} = a_i p_i - p_{i+1}.$$

Since the $\gcd(p, p') = 1$, this procedure eventually terminates with the relation

$$p_{n-1} = a_n p_n - 0$$

where p_n is a scalar (since it is a scalar multiple of $\gcd(p, p') = 1$).

For each real number a, consider the sequence

$$p_0(a), p_1(a), \ldots, p_{n-1}(a), p_n(a).$$

We say a sign change occurs at p_i and a, if $p_i(a)p_{i+1}(a) < 0$; i.e., $p_i(a)$ is positive and $p_{i+1}(a)$ or vice versa. We also say a sign change occurs at p_i and a if $p_{i-1}(a) > 0$, $p_i(a) = 0$, and $p_{i+1}(a) < 0$, or if $p_{i-1}(a) < 0$, $p_i(a) = 0$, and $p_{i+1}(a) > 0$. In fact, the proof below will show that if $p_i(a) = 0$, then $p_{i-1}(a)p_{i+1}(a) < 0$; so there is always a sign change at p_i and a.

If a sign change occurs at p_i and a, we write $\chi_i(a) = 1$; otherwise we write $\chi_i(a) = 0$. Let

$$\chi(a) = \chi_0(a) + \cdots + \chi_{n-1}(a);$$

in other words, $\chi(a)$ is the total number of sign changes in the sequence $p_0(a)$, $p_1(a)$, $\ldots$, $p_n(a)$.

6.8.2 Sturm's Theorem. *Let $p(x) \in \mathbb{R}[x]$ be a polynomial with simple roots. Then the number of real roots in the interval $[a, b]$ is $\chi(a) - \chi(b)$.*

Proof. Since $\gcd(p_i, p_{i+1}) = 1$, the polynomials p_i and p_{i+1} have no common roots. If $p_k(t) = 0$, then

$$p_{k-1}(t) = a_k p_k(t) - p_{k+1}(t) = -p_{k+1}(t).$$

From this, we can deduce that if $p_k(t) = 0$, then $p_{k\pm1}$ are non-zero and of opposite signs in a neighbourhood of t. The constant function p_n never changes sign. Moreover, the roots of p_0 are simple, so p_0 changes sign at each root.

Consider the effect on the function χ_0 near a root t of p_0. Note that a sign change in p_0 does not effect χ_k for $k \geq 1$, as these quantities do not depend on p_0. Since t is a simple root, p_0 changes sign at t. Suppose that the sign change of p_0 is from positive to negative. Then p_0 is decreasing near t, and thus the derivative p_1 is negative near t. So there is a sign change from positive to negative between p_0 and p_1 on the interval $(t-\varepsilon, t)$, but no change (from negative to negative) on the interval $(t, t+\varepsilon)$ for small $\varepsilon > 0$. In other words, the function χ_0 decreases by one at t:

$$\lim_{\varepsilon \to 0^+} \chi_0(t+\varepsilon) - \chi_0(t-\varepsilon) = -1.$$

Similarly, if p_0 changes sign from negative to positive at t, then p_0 is increasing, and p_1 is positive near t. So again there is a sign change between p_0 and p_1 on the interval $(t-\varepsilon, t)$, but no change on the interval $(t, t+\varepsilon)$ for small $\varepsilon > 0$. So again the function χ_0 decreases by one at t.

Next consider the effect of a zero t of p_k for $1 \le k < n$. The resulting (possible) change of sign of p_k may affect both χ_{k-1} and χ_k. As shown above, $p_{k\pm1}$ are of opposite signs in a neighbourhood of t. Now

$$\gcd(p_{k-1}, p_k) = 1 = \gcd(p_k, p_{k+1}),$$

and thus p_k has no roots in common with $p_{k\pm1}$. Hence there exists $\epsilon > 0$ for which $p_{k\pm1}$ are non-zero on $[t-\varepsilon, t+\varepsilon]$ and p_k has only t as a root in this interval. So, we may assume without loss of generality that $p_{k-1} < 0$ and $p_{k+1} > 0$ on $[t-\epsilon, t+\epsilon]$. Observe that a change of signs is possible for p_k at t. We make the following table

	p_{k-1}	p_k	p_{k+1}
$t-\epsilon$	$-$	?	$+$
t	$-$	0	$+$
$t+\epsilon$	$-$	?	$+$

where we do not know the signs of $p_k(t \pm \epsilon)$. Changing the sign from $-$ to $+$ results in increasing $\chi_{k-1}(t+\varepsilon)$ by 1 and decreasing $\chi_k(t+\varepsilon)$ by 1, leaving $\chi_{k-1}(t\pm\varepsilon) + \chi_k(t\pm\varepsilon)$ the same. Similarly a change from $+$ to $-$ results in decreasing $\chi_{k-1}(t+\varepsilon)$ by 1 and increasing $\chi_k(t+\varepsilon)$ by 1, again leaving $\chi_{k-1}(t\pm\varepsilon) + \chi_k(t\pm\varepsilon)$ the same. Of course, if the sign of p_k does not change, this also has no effect on $\chi(t\pm\varepsilon)$. A sign change in p_k does not affect χ_j except for $j = k-1$ and k. Therefore regardless of these signs, we see $\chi(t-\epsilon) = \chi(t+\epsilon)$.

The theorem now follows. Our above analysis proves that $\chi(a) - \chi(b) = \chi_0(a) - \chi_0(b)$. So if $\chi(a) - \chi(b) = n$, this must be a result of a decrease of 1 in the value of χ_0 at each of n zeros of p_0 between a and b. ■

6.8.3. Example. Consider the polynomial $p(x) = x^5 - 3x - 1$. One checks that $\gcd(p, p') = \gcd(x^5 - 3x - 1, 5x^4 - 3) = 1$, so that p has simple roots. Then

$$\begin{aligned}
p_1(x) &= 5x^4 - 3 \\
p_2(x) &= \frac{x}{5}p_1(x) - p(x) = \frac{12}{5}x + 1 \\
p_3(x) &= \Big(\frac{5^2}{12}x^3 - \frac{5^3}{12^2}x^2 + \frac{5^4}{12^3}x - \frac{5^5}{12^4}\Big)p_2(x) - p_1(x) \\
&= \frac{4^4 3^5 - 5^5}{12^4} > 0.
\end{aligned}$$

Consider the following table of signs.

This chart shows that there are three real roots. One lies in each of the intervals $(-2,-1)$, $(-1,0)$ and $(1,2)$. We could refine this by checking the points $-1.9, -1.8, \ldots, -1.1$, etc., to get more detail.

Exercises

1. Use Sturm's algorithm to find the number of zeros of $x^7 - 7x^3 + 8$.

	p	p_1	p_2	p_3	
x	x^5-3x-1	$5x^4-3$	$12x+5$	1	χ
$-\infty$	$-$	$+$	$-$	$+$	3
-2	$-$	$+$	$-$	$+$	3
-1	$+$	$+$	$-$	$+$	2
0	$-$	$-$	$+$	$+$	1
1	$-$	$+$	$+$	$+$	1
2	$+$	$+$	$+$	$+$	0
$+\infty$	$+$	$+$	$+$	$+$	0

TABLE 6.8.1. sign changes

2. Use Sturm's algorithm to show that x^3+ax+b has three real roots (counting multiplicity) if and only if

$$\Delta := -4a^3-27b^2 \geq 0.$$

Remember to deal with the case of repeated roots separately.

3. Solve the previous two exercises using calculus. (For simple polynomials like these, calculus is easier.)

4. Locate all 7 roots of $x^7-259x^5-510x^4+2x^3-518x-1020$ within 0.5 using Sturm's algorithm.

5. Use Sturm's algorithm to locate all real roots of x^6-5x^3+2x-1 up to an error of 0.1.

6. If $f \in \mathbb{R}[x]$ has repeated roots, explain how to factor f into a product of polynomials with simple roots.

6.9. Symmetric Functions

Consider the polynomial

$$\begin{aligned}\prod_{i=1}^{n}(x-y_i) &= x^n-(y_1+y_2+\ldots+y_n)x^{n-1}+\ldots\pm y_1y_2\ldots y_n\\ &= x^n-P_1(y_1,y_2,\ldots,y_n)x^{n-1}+\ldots\pm P_n(y_1,y_2,\ldots,y_n)\\ &= x^n+\sum_{i=1}^{n}(-1)^iP_i(y_1,y_2,\ldots,y_n)x^{n-i}.\end{aligned}$$

The coefficients of x^i are special polynomials in $\{y_1, y_2, \ldots, y_n\}$.

$$\begin{array}{rcll} P_1 & = & \sum_{i=1}^n y_i & = \; y_1 + y_2 + \ldots + y_n \\ P_2 & = & \sum_{i<j} y_i y_j & = \; y_1y_2 + y_1y_3 + \ldots + y_{n-1}y_n \\ & \vdots & & \\ P_k & = & \sum_{i_1<i_2<\ldots i_k} y_{i_1} y_{i_2} \ldots y_{i_k} & \\ & \vdots & & \\ P_n & = & \prod_{i=1}^n y_i & = \; y_1y_2 \ldots y_n \end{array}$$

The values of these polynomials are not changed if the y_i's are permuted. In general, a function of several variables is called **symmetric** if it is invariant under permutation of the variables. That is to say, for every permutation π of $\{1, 2, \ldots, n\}$,

$$f(y_{\pi(1)}, y_{\pi(2)}, \ldots, y_{\pi(n)}) = f(y_1, y_2, \ldots, y_n).$$

Moreover, each of these polynomials is homogeneous. A polynomial $p \in \mathbb{F}[y_1, \ldots, y_n]$ is called **homogeneous** of degree k if

$$p(ty_1, ty_2, \ldots, ty_n) = t^k p(y_1, y_2, \ldots, y_n) \quad \text{for} \quad t \in \mathbb{F}.$$

Notice that P_k is homogeneous of degree k for $1 \leq k \leq n$.

The functions P_1, P_2, ..., P_n are called **elementary symmetric polynomials**. The rather surprising fact is that every symmetric polynomial in n variables can be expressed uniquely as a polynomial in $P_1, \ldots, P_n$. Let us look at an example.

6.9.1. Example. For $n = 3$, the elementary symmetric polynomials are

$$\begin{aligned} P_1 &= y_1 + y_2 + y_3 \\ P_2 &= y_1y_2 + y_1y_3 + y_2y_3 \\ P_3 &= y_1y_2y_3. \end{aligned}$$

Consider the symmetric polynomial

$$\begin{aligned} p &= 2\sum_{i=1}^3 y_i^3 - 3\sum_{i\neq j} y_i^2 y_j + 12y_1y_2y_3 \\ &= 2(y_1^3 + y_2^3 + y_3^3) - 3(y_1^2y_2 + y_1^2y_3 + y_2^2y_1 + y_2^2y_3 + y_3^2y_1 + y_3^2y_2) + 12y_1y_2y_3 \end{aligned}$$

This is perhaps the natural way to write down a symmetric polynomial, by collecting together all monomials of the same type. So for $n = 3$ and

polynomials homogeneous of degree 3, there are the three polynomials

$$\begin{aligned} q_1 &= \sum_{i=1}^{3} y_i^3 \\ q_2 &= \sum_{i \neq j} y_i^2 y_j \\ q_3 &= y_1 y_2 y_3. \end{aligned}$$

So $p = 2q_1 - 3q_2 + 12q_3$.

Let us compute the symmetric polynomials homogeneous of degree 3 which can be obtained as monomials in P_1, P_2 and P_3. They are

$$\begin{array}{lcll} P_1^3 & = & (y_1 + y_2 + y_3)^3 & = & q_1 + 3q_2 + 6q_3 \\ P_1 P_2 & = & (y_1 + y_2 + y_3)(y_1 y_2 + y_1 y_3 + y_2 y_3) & = & q_2 + 3q_3 \\ P_3 & = & y_1 y_2 y_3 & = & q_3 \end{array}$$

Notice that only P_1^3 contains the term y_1^3, and so is the only one which requires q_1 in its expression. After subtracting $2P_1^3$ from p, the polynomial is a combination of q_2 and q_3. Of the remaining two terms, only $P_1 P_2$ contains the term $y_1^2 y_2$, and hence requires q_2 in its expression. So a multiple of $P_1 P_2$ can be subtracted off leaving a multiple of $q_3 = P_3$.

We can use vector notation to simplify the calculation involved. Since

$$(2, -3, 12) = 2(1, 3, 6) - 9(0, 1, 3) + 27(0, 0, 1),$$

we obtain the relation

$$p = 2P_1^3 - 9P_1 P_2 + 27P_3.$$

6.9.2. Theorem. *Every symmetric polynomial in n variables with coefficients in a field $\mathbb{F}$ can be expressed uniquely as a polynomial with coefficients in $\mathbb{F}$ in the n elementary symmetric polynomials.*

Proof. The example basically explains how to proceed in general. We proceed by induction. Given a symmetric polynomial $p(y_1, y_2, \ldots, y_n)$, let m be the largest degree of any monomial in p. Choose the term of degree m so that the power of y_1 is as large as possible, and after that, the power of y_2 is as large as possible, and so on. Thus p contains a term

$$a y_1^{k_1} y_2^{k_2} \ldots y_n^{k_n}$$

where $k_1 \geq k_2 \geq \ldots > k_n$ and $k_1 + k_2 + \ldots + k_n = m$. Call this the 'largest' term in p.

We assume the induction hypothesis that the theorem holds for symmetric polynomials of lower degree, and for polynomials of the same degree such that the largest term

$$b y_1^{j_1} y_2^{j_2} \ldots y_n^{j_n}$$

precedes that of p in the lexicographic order on the exponents. That is, we say that $(j_1, \ldots, j_n) \prec (k_1, \ldots, k_n)$ if $j_1 < k_1$ or $j_i = k_i$ for $1 \leq i < i_0$ and $j_{i_0} < k_{i_0}$.

The idea is to write down the monomial in $P_1, \ldots, P_n$ which has the same largest term and subtract off an appropriate multiple. It is not too hard to see that this polynomial is precisely

$$P = P_1^{k_1-k_2} P_2^{k_2-k_3} \ldots P_n^{k_n}.$$

This is because the 'largest' term of P is the product of the 'largest' terms of each factor, namely

$$y_1^{k_1-k_2}(y_1y_2)^{k_2-k_3} \ldots (y_1y_2 \ldots y_n)^{k_n}.$$

Indeed, the exponent of y_i in this product is

$$(k_i - k_{i+1}) + (k_{i+1} - k_{i+2}) + \ldots + (k_{n-1} - k_n) + k_n = k_i.$$

Now the polynomial $p - aP$ has a smaller 'largest' term. So by the induction hypothesis, it can be expressed uniquely as a polynomial in the elementary symmetric polynomials. Adding the monomial aP to this yields a polynomial expression in P_1, ..., P_n for p as well. This expression is unique since there was a unique choice, aP, of a symmetric function with the same largest term as p and having removed that, there is a unique expression for the remainder. ■

The most important use of symmetric functions is based on the fact that the coefficients of a polynomial are precisely the elementary symmetric functions of the roots. This should be clear from their definition, but it bears repeating. The monic polynomial with roots r_1, ..., r_n is

$$p(x) = \prod_{i=1}^{n}(x - r_i) = x^n + \sum_{i=1}^{n}(-1)^i P_i(r_1, r_2, \ldots, r_n)x^{n-i}.$$

In particular, if $q = x^n + q_{n-1}x^{n-1} + \ldots + q_1x + q_0$ is an irreducible polynomial in $\mathbb{Q}[x]$, so that r_1, ..., r_n are all algebraic conjugates, we see that the elementary symmetric functions of the roots are *rational*

$$P_i(r_1, \ldots, r_n) = (-1)^i q_i.$$

Thus Theorem 6.9.2 implies that every symmetric function of these roots with coefficients in $\mathbb{Q}$ is rational.

This provides one way of proving the following result.

6.9.3. Theorem. *The algebraic numbers form a field.*

Proof. It must be shown that if α and β are algebraic numbers, then so are $\alpha+\beta$, $\alpha\beta$ and $1/\alpha$. It was shown in section 6.6, exercise 4 that the reciprocal of algebraic numbers are algebraic. The method for sums and products are similar. So only sums will be done here.

Let p and q be irreducible polynomials in $\mathbb{Q}[x]$ with α and β as roots. Let $\alpha_1, \ldots, \alpha_m$ be the roots of p; and let $\beta_1, \ldots, \beta_n$ be the roots of q. It is enough to show that the polynomial with roots $\alpha_i + \beta_j$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ has rational coefficients. However, we know that if $P_1, \ldots, P_{nm}$ are the elementary polynomials in nm variables, then

$$r(x) = \prod_{1 \leq i \leq m} \prod_{1 \leq j \leq n} (x - \alpha_i - \beta_j) = \sum_{k=0}^{nm} (-1)^k P_k(\alpha_i + \beta_j) x^k$$

where $P_k(\alpha_i + \beta_j)$ is a symmetric function of the mn roots $\alpha_i + \beta_j$. Thus, thinking of this as a function of the β_j, it is a symmetric polynomial with coefficients that are symmetric functions of the α_i with rational coefficients. Therefore, these coefficients are themselves rational. Thus $P_k(\alpha_i + \beta_j)$ is reduced to a symmetric polynomial in the β_j with rational coefficients. So it is a rational number.

We conclude that $r \in \mathbb{Q}[x]$, and hence its roots are all algebraic. In particular, $\alpha + \beta$ is algebraic. ■

Exercises

1. Express $x_1^4 + x_2^4 + x_3^4$ as a polynomial in the three elementary symmetric polynomials in three variables.

2. Verify that if α and β are algebraic numbers, then so is $\alpha\beta$.

3. Let $\alpha = \sqrt{3}$ and $\beta = \sqrt[3]{7}$.
(a) Find a monic polynomial q of degree 6 in $\mathbb{Q}[x]$ with $\alpha + \beta$ as a root.
(b) Show that $\gamma_{j,k} := (-1)^j \alpha + \omega^k \beta$ are also roots of q for $j \in \{0, 1\}$, $k \in \{0, 1, 2\}$ and $\omega = \frac{-1+i\sqrt{3}}{2}$.
(c) Check that $P_2(\gamma_{00}, \ldots, \gamma_{1,2})$ is the coefficient of x^2 in q.

4. **(Newton–Girard identities)** Fix an integer $n \geq 2$. For each $k \geq 0$, let $q_k = \sum_{i=1}^n x_i^k$, which is known as a *power sum*. Let $P_0, \ldots, P_n$ denote the elementary symmetry symmetric functions in $x_1, \ldots, x_n$. Since the q_k are symmetric, they are expressible in terms of the P_i. Prove the following explicit formula:

$$q_k = (-1)^k k \sum_{r_1 + 2r_2 + \cdots + kr_k = k} \frac{(r_1 + \cdots + r_k - 1)!}{r_1! \ldots r_k!} \prod_{i=1}^{k} (-P_i)^{r_i}.$$

5. Let the *complete Bell Polynomials* be defined recursively by $B_0 = 1$ and

$$B_{k+1}(x_1, \ldots, x_{k+1}) = \sum_{i=0}^{k} \binom{k}{i} B_{k-i}(x_1, \ldots, x_{k-i}) x_{i+1}.$$

Prove

$$B_k(x_1, \ldots, x_k) = \left(\frac{d}{dt}\right)^k \exp\left(\sum_{i=1}^{k} x_i \frac{t^i}{i!}\right).$$

6. (Express elementary symmetric polynomials using power sums) Use the notation of Exercise 4.

(a) Prove that the elementary symmetric functions are expressible as polynomials with rational coefficients in the power sums. Specifically, prove

$$P_k = \frac{(-1)^k}{k!} B_k(-q_1, -(1!)q_2, -(2!)q_3, \ldots, -(k-1)!q_k).$$

(b) Conclude that every symmetric polynomial with rational coefficients is expressible as a polynomial in the power sums.

7. Prove that the elementary symmetric polynomials are not expressible as polynomials with *integer* coefficients in the power sums.

6.10. Cubic Polynomials

In this section, we will show how to use the power of symmetric polynomials to factor cubic equations in $\mathbb{C}[x]$. It is nice to know that there is such a formula, although it is too complicated to be of much practical use. In particular, even when all three roots are real, the formula still requires complex numbers.

To illustrate the idea in a more simple setting, first consider a quadratic polynomial $x^2 + ax + b$. Let the two roots be r_1 and r_2. We know that

$$\begin{array}{rcccr} r_1 + r_2 & = & P_1(r_1, r_2) & = & -a \\ r_1 r_2 & = & P_2(r_1, r_2) & = & b \end{array}$$

The symmetric function of the roots $(r_1 - r_2)^2$ is given by

$$(r_1 - r_2)^2 = (r_1 + r_2)^2 - 4r_1 r_2 = a^2 - 4b.$$

Hence

$$\begin{array}{rcccr} r_1 & = & \frac{1}{2}\big((r_1 + r_2) + (r_1 - r_2)\big) & = & \dfrac{-a + \sqrt{a^2 - 4b}}{2} \\ r_2 & = & \frac{1}{2}\big((r_1 + r_2) - (r_1 - r_2)\big) & = & \dfrac{-a - \sqrt{a^2 - 4b}}{2} \end{array}$$

For cubics, the same kind of technique works, although it is a fair bit more complicated. The first simplifying step is to make a change of variables to eliminate the coefficient of x^2. This is analogous to completing the square in the quadratic case. Suppose we are given a cubic polynomial

$$w^3 + Aw^2 + Bw + C.$$

Make the substitution $w = x - A/3$. Then we obtain a polynomial

$$(x - A/3)^3 + A(x - A/3)^2 + B(x - A/3) + C = x^3 + ax + b$$

where $a = B - A^2/3$ and $b = C - AB/3 + 2A^3/27$. If we can find the roots x_1, x_2 and x_3 of this cubic, then the roots of the original are $w_i = x_i - A/3$. The elementary functions in the x_i are

$$\begin{array}{rcll} P_1 & = & x_1 + x_2 + x_3 & = & 0 \\ P_2 & = & x_1x_2 + x_1x_2 + x_2x_3 & = & a \\ P_3 & = & x_1x_2x_3 & = & -b \end{array}$$

The idea is to look for some 'almost symmetric' functions y_i of the roots which are roots of $y^3 = d$ for some d. We investigate the properties such a y must have. Let D represent a cube root of d and let $\omega = e^{2\pi i/3}$ be a cube root of 1. Then

$$y^3 - D^3 = (y - D)(y - \omega D)(y - \omega^2 D).$$

This suggests writing down the following functions of the roots x_1, x_2 and x_3. (This change of coordinates is known as a discrete Fourier transform.)

$$\begin{array}{rcll} y_1 & = & & x_1 + \omega x_2 + \omega^2 x_3 \\ y_2 & = & \omega y_1 & = & \omega x_1 + \omega^2 x_2 + x_3 \\ y_3 & = & \omega^2 y_1 & = & \omega^2 x_1 + x_2 + \omega x_3 \\ z_1 & = & & x_1 + \omega^2 x_2 + \omega x_3 \\ z_2 & = & \omega^2 z_1 & = & \omega^2 x_1 + \omega x_2 + x_3 \\ z_3 & = & \omega z_1 & = & \omega x_1 + x_2 + \omega^2 x_3 \end{array}$$

We find that

$$y_1^3 = y_2^3 = y_3^3 = y_1y_2y_3$$
$$z_1^3 = z_2^3 = z_3^3 = z_1z_2z_3$$

and

$$y_1z_1 = y_2z_2 = y_3z_3.$$

For convenience, write the subscripts mod 3 (so that x_4 means x_1). A computation shows that

$$y_1^3 = \sum_{i=1}^{3} x_i^3 + 3\omega \sum_{i=1}^{3} x_i^2x_{i+1} + 3\omega^2 \sum_{i=1}^{3} x_ix_{i+1}^2 + 6x_1x_2x_3$$
$$z_1^3 = \sum_{i=1}^{3} x_i^3 + 3\omega^2 \sum_{i=1}^{3} x_i^2x_{i+1} + 3\omega \sum_{i=1}^{3} x_ix_{i+1}^2 + 6x_1x_2x_3$$

Neither of these is symmetric, but their sum is,

$$\begin{aligned} y_1^3 + z_1^3 &= 2\sum_{i=1}^{3} x_i^3 - 3\sum_{i=1}^{3} x_i^2 x_{i+1} - 3\sum_{i=1}^{3} x_i x_{i+1}^2 + 12x_1x_2x_3 \\ &= 2\Big(\big(\sum_{i=1}^{3} x_i\big)^3 - 3\sum_{i\neq j} x_i^2 x_j - 6x_1x_2x_3\Big) - 3\sum_{i\neq j} x_i^2 x_j + 12P_3 \\ &= 2(P_1^3 - 6P_3) - 9\Big(\big(\sum_{i=1}^{3} x_i\big)\big(\sum_{i\neq j} x_i x_j\big) - 3x_1x_2x_3\Big) + 12P_3 \\ &= 2P_1^3 - 9P_1P_2 + 27P_3 = -27b. \end{aligned}$$

Notice the big advantage of simplicity in this formula occurs because $P_1 = 0$.

Similarly, compute

$$\begin{aligned} y_1 z_1 &= \sum_{i=1}^{3} x_i^2 + (\omega + \omega^2) \sum_{1\le i<j\le 3} x_i x_j \\ &= \sum_{i=1}^{3} x_i^2 - \sum_{1\le i<j\le 3} x_i x_j \\ &= \Big(\sum_{i=1}^{3} x_i\Big)^2 - 3\sum_{1\le i<j\le 3} x_i x_j \\ &= P_1^2 - 3P_2 = -3a. \end{aligned}$$

Hence y_1, y_2, y_3, z_1, z_2 and z_3 are the roots of

$$\begin{aligned} (X^3 - y_1^3)(X^3 - z_1^3) &= X^6 - (y_1^3 + z_1^3)X^3 + (y_1z_1)^3 \\ &= X^6 + 27bX^3 - 27a^3. \end{aligned}$$

This is a quadratic in X^3, and thus it can be solved:

$$X^3 = \frac{-27b \pm \sqrt{27(27b^2 + 4a^3)}}{2}.$$

Because of the symmetry involved, we can let y_1 be any cube root

$$y_1 = \sqrt[3]{\frac{-27b + \sqrt{27(27b^2 + 4a^3)}}{2}}.$$

Then $z_1 = -3a/y_1$. So from the equations for y_1 and z_1, we obtain

$$y_1 + z_1 = 2x_1 - x_2 - x_3 = 3x_1 - P_1.$$

Thus the roots of the cubic $x^3 + ax + b$ are

$$\begin{aligned} x_1 &= y_1/3 - a/y_1 \\ x_2 &= \omega y_1/3 - \omega^2 a/y_1 \\ x_3 &= \omega^2 y_1/3 - \omega a/y_1. \end{aligned}$$

To get the roots of the original cubic, add $-A/3$.

6.10.1. Example. Consider the polynomial $x^3 - 7x + 6$, which you can factor by hand using the rational root theorem, but has the virtue of being computable by hand in our formula. We have

$$\begin{aligned} y_1 &= \sqrt[3]{\frac{-27(6) + \sqrt{27(27(6)^2 + 4(-7)^3)}}{2}} \\ &= \sqrt[3]{-81 + 3\sqrt{729 - 1029}} \\ &= \sqrt[3]{-81 + 30\sqrt{3}i} = 3 + 2\sqrt{3}i \end{aligned}$$

Now, for future convenience, compute

$$-\frac{a}{y_1} = \frac{7\overline{y_1}}{|y_1|^2} = \frac{3 - 2\sqrt{3}i}{3}.$$

Plugging this in to the formulae, we obtain

$$\begin{aligned} x_1 &= \frac{3 + 2\sqrt{3}i + 3 - 2\sqrt{3}i}{3} &&= 2 \\ x_2 &= \frac{(-1 + \sqrt{3}i)(3 + 2\sqrt{3}i) + (-1 - \sqrt{3}i)(3 - 2\sqrt{3}i)}{6} &&= -3 \\ x_3 &= \frac{(-1 - \sqrt{3}i)(3 + 2\sqrt{3}i) + (-1 + \sqrt{3}i)(3 - 2\sqrt{3}i)}{6} &&= 1 \end{aligned}$$

Even for such a nice cubic, the calculations are daunting. However, this formula has the virtue of providing a closed form, algebraic expression for the roots. For finding approximate values of the roots, numerical methods based on calculus are much superior. Those methods, however, do not provide exact solutions.

Exercises

1. Redo Exercise 2 from Section 6.8 without using Sturm's algorithm.

2. Find the roots of $x^3 - 6x + 9$.

3. Find the roots of $x^3 - 15x^2 + 60x - 54$.

4. Show that $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2} = 1$.

5. A sphere with outer radius r which is 1 cm. thick has the same volume in the shell as in the interior hole. Find r.

6. (Cubic resolvent) If f is a degree n polynomial with roots $r_1, \ldots, r_n$, its *discriminant* is defined to be

$$\Delta(f) = \prod_{i<j} (r_i - r_j)^2.$$

The *cubic resolvent* of a quartic polynomial $x^4 + ax^3 + bx^2 + cx + d$ is defined to be the polynomial $x^3 - bx^2 + (ac - 4d)x - (a^2d + c^2 - 4bd)$. The cubic resolvent plays an important role in solving quartic equations. Prove that a quartic polynomial and its cubic resolvent have the same discriminant.

Notes on Chapter 6

The formula for the roots of a cubic was discovered by the Italian mathematicians del Ferro and Tartaglia in early 16th century. Cardano and his student Ferrari learned Tartaglia's method, and found a solution for the quartic. The formula for quartics is considerably more complicated than the cubic case. It was long an open problem whether such a solution could be obtained for arbitrary polynomial equations. In order for this to be the case, every algebraic number would have to be expressible as a combination of various k-th roots. However, in 1826, the Norwegian algebraist Abel published the first rigourous argument showing that there are polynomials of degree 5 which cannot be solved by repeated extraction of roots.

Remarkable progress was made shortly after, in 1831, by the young mathematician Galois, who died in a duel when he was 20. Galois showed that one can study the roots of a polynomial by looking at the structure of the field obtained by adding all of the roots of this polynomial to the rationals. The set of all isomorphisms of this field onto itself forms a group. The structure of this group can be used to decide if a polynomial can be 'solved by radicals', meaning that the roots can be expressed by extraction of roots. This is a very beautiful theory, and one of the landmarks of modern algebra.

It was not until Viète in the late 16th century and Descartes in the early 17th century that a good notation for polynomials was proposed. Stevin proved the Intermediate value theorem for polynomials, thereby showing that real polynomials of odd degree have a root. Descartes considered the graphs of polynomials. He found the rational root theorem and formulated his rule of signs, but did not publish his proof (as was common). He also observed that a polynomial of degree n has at most n roots. Newton showed that complex roots of real polynomials come in conjugate pairs. He also studied the symmetric functions of the roots and related them to the coefficients of a polynomial.

The fundamental theorem of algebra was discussed in the notes to the previous chapter.

Gauss's lemma comes from his early work in 1801. Eisenstein's criterion dates from 1850. Sturm published his algorithm in 1829. It was the first effective algebraic algorithm for locating roots of a polynomial to any accuracy. In 1901, Kronecker published a set of lectures which includes a statement and proof of unique factorization of (rational or integer) polynomials into irreducibles.

Liouville was the first to construct transcendental numbers in 1851. Hermite showed that e is transcendental in 1873, and Lindemann showed that π is transcendental in 1882.

The general algebra of polynomials can be found in various introductions to abstract algebra such as Artin [**5**]. Sturm's theorem and Descartes rule of signs can be found in [**38**] and [**28**]. Hardy and Wright [**15**] is a good source for information on algebraic and transcendental numbers; also see Stark [**37**] and Silverman [**34**]. See Gray [**14**] for more about the history.

Chapter 7

Finite Fields

This chapter contains a detailed study of finite fields. It tries to emphasize the dramatic parallels between the arithmetic of the integers modulo a prime and the corresponding arithmetic of polynomials modulo an irreducible polynomial. At the end of the chapter, we will obtain an algorithm for factoring integer polynomials efficiently on a computer, in contrast to the (apparent) difficulty of factoring large integers.

7.1. Arithmetic Modulo a Polynomial

If p is a polynomial in $\mathbb{F}[x]$, then it is possible to do calculations modulo p. As in the integer case, say that polynomials $a(x)$ and $b(x)$ in $\mathbb{F}[x]$ are congruent mod p if p divides $a - b$:

$$a \equiv b \pmod{p} \quad \text{if and only if} \quad p|(a-b).$$

This yields a ring of equivalence classes, analogous to the rings $\mathbb{Z}_n$, called $\mathbb{F}[x]/(p)$. The point is that addition and multiplication of equivalence classes are well defined because of the following proposition. The proof is left as an exercise. (Compare with Proposition 2.1.1.)

7.1.1. Proposition. *Let p, a_i and b_i be polynomials in $\mathbb{F}[x]$ such that*

$$a_1 \equiv a_2 \pmod{p} \quad \textit{and} \quad b_1 \equiv b_2 \pmod{p}.$$

Then

(1) $a_1 + b_1 \equiv a_2 + b_2 \pmod{p}$.
(2) $a_1 b_1 \equiv a_2 b_2 \pmod{p}$.

This means that addition and multiplication of equivalence classes can be defined by

$$[a] + [b] = [a + b] \quad \text{and} \quad [a][b] = [ab].$$

One may verify the various properties of a commutative ring, such as associativity of addition and multiplication, and the distributive law, because these properties hold for the ring $\mathbb{F}[x]$.

7.1.2. Example. Consider the ring $S = \mathbb{R}[x]/(x^2+1)$. By the division algorithm, every polynomial q is equivalent modulo x^2+1 to its remainder after division by x^2+1, which is a linear polynomial $a+bx$. Since the only linear polynomial divisible by x^2+1 is 0, each linear polynomial belongs to a different equivalence class. Thus

$$S = \{[a+bx] : a, b \in \mathbb{R}\}.$$

Addition and multiplication are given by

$$[a+bx] + [c+dx] = [(a+c) + (b+d)x]$$

$$\begin{aligned}[a+bx][c+dx] &= [ac + (ad+bc)x + bdx^2] \\ &= [(ac-bd) + (ad+bc)x].\end{aligned}$$

A moment's reflection will show that this corresponds to the rules of multiplication in the complex numbers $\mathbb{C}$.

This correspondence is not a coincidence. Notice that $\pm i$ are the two roots of the irreducible polynomial x^2+1. In S, the equation $X^2+1=0$ has the solution $[x]$. That is why $[x]$ takes the place of i. We can define a map φ from $\mathbb{R}[x]$ into $\mathbb{C}$ by $\varphi(q) = q(i)$. One may check that φ preserves addition and multiplication. Moreover, $\varphi(q) = 0$ if and only if i is a root of q. By Theorem 6.6.2, it follows that q is divisible by the minimal polynomial of i, namely x^2+1. Thus $\varphi(q) = 0$ if and only if $[q] = 0$ in S. So there is an **induced map** $\tilde{\varphi} : S \to \mathbb{C}$ given by $\tilde{\varphi}([q]) = q(i)$ as in Lemma 6.1.4. The point of the previous discussion is two-fold. First $\tilde{\varphi}$ is well defined because $q_1 \equiv q_2 \pmod{x^2+1}$ implies that $q_1(i) = q_2(i)$. Secondly, $\tilde{\varphi}$ is one-to-one because $q_1(i) = q_2(i)$ implies that $x^2+1 | (q_1 - q_2)$; i.e. $q_1 \equiv q_2 \pmod{x^2+1}$. So $\tilde{\varphi}$ maps S one-to-one and onto $\mathbb{C}$, and preserves all the operations (addition, multiplication, 0, 1). Therefore $\tilde{\varphi}$ is a ring isomorphism. (Recall Definition 1.1.2.) This means that they represent the same mathematical object.

The complex numbers form a field. The ring isomorphism $\tilde{\varphi}$ can be used to show that S is also a field. For any $s \neq 0$, let $z = \tilde{\varphi}(s)$. Since $\tilde{\varphi}$ is one-to-one, $z \neq 0$. So $z^{-1} \in \mathbb{C}$. Since $\tilde{\varphi}$ is onto, $t = \tilde{\varphi}^{-1}(z^{-1}) \in S$ and

$$st = \tilde{\varphi}^{-1}(z)\tilde{\varphi}^{-1}(z^{-1}) = \tilde{\varphi}^{-1}(1) = 1.$$

That is, $t = s^{-1}$. Therefore S is a field.

The polynomial x^2+1 is irreducible in $\mathbb{R}[x]$, and the quotient ring S turned out to be a field. This is completely analogous to the fact that $\mathbb{Z}_n$ is a field if and only if n is prime.

7.1.3. Proposition. *$\mathbb{F}[x]/(p)$ is a field if and only if p is irreducible. If p is reducible, then $\mathbb{F}[x]/(p)$ has zero divisors.*

Proof. If p is not irreducible in $\mathbb{F}[x]$, then it factors as $p = ab$ where both a and b have positive degree. Since p does not divide either a or b, the equivalence classes $[a]$ and $[b]$ in $\mathbb{F}[x]/(p)$ are non-zero. However,

$$[a][b] = [p] = [0].$$

So $\mathbb{F}[x]/(p)$ has zero divisors.

On the other hand, if p is irreducible, and $[a] \neq [0]$, then $\gcd(a, p) = 1$. Thus by the Euclidean algorithm for polynomials 6.2.4, there are polynomials s and t in $\mathbb{F}[x]$ so that $1 = as + pt$. Hence

$$[a][s] = [1 - pt] = [1].$$

Therefore, all non-zero elements of $\mathbb{F}[x]/(p)$ are units, and so it is a field. ■

The significance of this construction comes from the fact that it provides a method for constructing a bigger field containing $\mathbb{F}$ in which p had a root. Let us record this as a theorem.

7.1.4. Theorem. *If $p \in \mathbb{F}[x]$ is irreducible, then the field $\mathbb{G} = \mathbb{F}[x]/(p)$ contains $\mathbb{F}$ as a subfield, and p has a root in $\mathbb{G}$.*

Proof. Notice that $\mathbb{F}$ sits inside $\mathbb{G}$ as the constant polynomials $[a]$ for $a \in \mathbb{F}$. The element $[x]$ is a root of p in $\mathbb{G}$ because

$$p([x]) = \sum_{i=0}^{d} p_i [x]^i = [p(x)] = [0].$$ ■

You may have noticed that modding out by p makes $[x]$ a root by fiat. This is precisely the rationale for doing this operation at all.

Exercises

1. Prove Proposition 7.1.1.

2. (a) Show that $x^5 + 7x^2 - 7 \in \mathbb{Z} - x]$ is irreducible.
(b) Find the inverse of $[x^2 + 3x - 1]$ in $\mathbb{Q}[x]/(x^5 + 7x^2 - 7)$.

3. (a) Show that $x^2 + 1$ is irreducible in $\mathbb{Z}_7[x]$.
(b) Find the smallest integer k so that $[2x]^k = 1$ in $\mathbb{Z}_7[x]/(x^2 + 1)$.
(c) How many elements are there in $\mathbb{Z}_7[x]/(x^2 + 1)$?

4. (a) Show that if d is a square-free positive integer, then $\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} : r, s \in \mathbb{Q}\}$ is a field.
(b) Express this field as a quotient ring of $\mathbb{Q}[x]$.

5. (a) Find an irreducible polynomial $p \in \mathbb{Z}[x]$ with $\sqrt{3} + \sqrt[3]{7}$ as a root.
(b) Show that $\mathbb{Z}[x]/(p)$ is a ring contained in the field $\mathbb{Q}[x]/(p)$.

6. Show that $\mathbb{Z}_p[x]/(x^4 + x^3 + x + 1)$ is not a field for any prime p.

7. (a) Show that if $a_1, a_2, p_1, p_2 \in \mathbb{F}[x]$ and $\gcd(p_1, p_2) = 1$, then the system

$$\begin{aligned} q &\equiv a_1 \pmod{p_1} \\ q &\equiv a_2 \pmod{p_2} \end{aligned}$$

has a unique solution $\pmod{p_1 p_2}$.
(b) Prove the Chinese Remainder Theorem for arithmetic modulo polynomials; i.e., if $\gcd(p_i, p_j) = 1$ whenever $1 \le i < j \le n$, show that

$$\begin{aligned} q &\equiv a_1 \pmod{p_1} \\ &\vdots \\ q &\equiv a_n \pmod{p_n} \end{aligned}$$

has a unique solution modulo $p_1 p_2 \cdots p_n$.

8. Suppose that $a_1, a_2, p_1, p_2, d \in \mathbb{F}[x]$ and $\gcd(p_1, p_2) = d$ and $d \notin \mathbb{F}$. When does the system

$$\begin{aligned} q &\equiv a_1 \pmod{p_1} \\ q &\equiv a_2 \pmod{p_2} \end{aligned}$$

have solutions? What can you say about these solutions?

7.2. An Eight-Element Field

Consider the polynomial $p(x) = x^3 + x + 1$ in $\mathbb{Z}_2[x]$. It is irreducible because it has no roots, and has degree 3. Let us investigate the field $\mathbb{F}_8 = \mathbb{Z}_2[x]/(x^3 + x + 1)$. By the division algorithm, the different equivalence classes are again given by all polynomials of degree less than p, namely the quadratic polynomials $a + bx + cx^2$. There are 2 choices for each a, b, c, so there are $8 = 2^3$ elements in $\mathbb{F}_8$. The multiplication rules are given by the following table.

It is apparent from this table that every element has an inverse. For example, $[x + 1][x^2 + x] = [1]$. It would be difficult to find the compatible addition and multiplication tables for a field of 8 elements without this construction.

By Theorem 7.1.4, we see that the polynomial $X^3 + X + 1$ has a root $[x]$ in $\mathbb{F}_8$. In fact, it has three roots. A calculation using the table above shows that

$$\begin{aligned} ([x]^2)^3 + [x]^2 + 1 &= ([x^2][x^2 + x]) + [x^2] + 1 \\ &= [x^2 + 1 + x^2 + 1] = [0] \end{aligned}$$

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

TABLE 7.2.1. Multiplication table for $\mathbb{F}_8$

So this yields the factorization

$$X^3 + X + 1 = (X - [x])(X - [x^2])(X - [x^2 + x]).$$

Now consider the powers of $[x]$ in $\mathbb{F}_8$. We have $[x]$, $[x^2]$, $[x^3] = [x + 1]$, $[x^4] = [x^2+x]$, $[x^5] = [x^2+x+1]$, $[x^6] = [x^2+1]$, and $[x^7] = 1$. So the powers of $[x]$ run through all the 7 non-zero elements of $\mathbb{F}_8$. This is a primitive root! Notice that for any non-zero $a \in \mathbb{F}_8$, there is a k so that $a = [x^k]$. So

$$a^7 = [x^7]^k = 1.$$

So a is a root of $X^7 - 1 = 0$. Since $7 = 8 - 1$, this is a variant of Fermat's little theorem for $\mathbb{F}_8$. We will establish this for all finite fields.

This means that $X^8 - X$ has 8 distinct roots in $\mathbb{F}_8$. So it factors into linear terms in $\mathbb{F}_8$:

$$X^8 - X = \prod_{a \in \mathbb{F}_8} (X - a).$$

Let us factor it in $\mathbb{Z}_2[X]$. A simple calculation shows that

$$X^8 - X = X(X - 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

The two cubics are irreducible in $\mathbb{Z}_2[X]$ because they have no roots in $\mathbb{Z}_2$. We saw above that $X^3 + X + 1$ factors into three linear terms in $\mathbb{F}_8[X]$. We now also can factor

$$X^3 + X^2 + 1 = (X - [x + 1])(X - [x^2 + 1])(X - [x^2 + x + 1]).$$

It turns out that there is only one field of order 8. This may seem surprising since there is a second irreducible polynomial of degree 3, namely $x^3 + x^2 + 1$. It turns out that this other choice leads to an equivalent field, in the sense that there is an isomorphism of one onto the other, as in Example 7.1.2. Consider the other 8 element field, $\mathbb{G} = \mathbb{Z}_2[y]/(y^3 + y^2 + 1)$.

As an exercise, write out the multiplication table for $\mathbb{G}$. Notice that $[y]$ is a root of $X^3 + X^2 + 1$ in $\mathbb{G}$. But $\mathbb{F}_8$ also has roots of this polynomial; for example, $[x + 1]$ is a root.

Consider the map from $\mathbb{G}$ to $\mathbb{F}_8$ given by

$$\varphi([a + by + cy^2]) = [a + b(x + 1) + c(x + 1)^2] = [(a + b + c) + bx + cx^2].$$

This map is easily seen to be a bijection, for

$$\varphi([a_1 + b_1y + c_1y^2]) = \varphi([a_2 + b_2y + c_2y^2])$$

implies that $b_1 = b_2$, $c_1 = c_2$ and $a_1 + b_1 + c_1 = a_2 + b_2 + c_2$, whence $a_1 = a_2$.

More significantly, φ preserves addition and multiplication.

$$\begin{aligned}
&\varphi([a_1 + b_1y + c_1y^2]) + \varphi([a_2 + b_2y + c_2y^2]) \\
&= [(a_1 + b_1 + c_1) + b_1x + c_1x^2] + [(a_2 + b_2 + c_2) + b_2x + c_2x^2] \\
&= [(a_1 + a_2 + b_1 + b_2 + c_1 + c_2) + (b_1 + b_2)x + (c_1 + c_2)x^2] \\
&= \varphi([(a_1 + a_2) + (b_1 + b_2)y + (c_1 + c_2)y^2]
\end{aligned}$$

This show that φ preserves addition. Multiplication is more subtle, and uses the fact that $[y]$ and $[x+1]$ have the same minimal polynomial $q(X) = X^3 + X^2 + 1$. Hence $[y^3] = [y^2 + 1]$ and $[y^4] = [y^2 + y + 1]$ and likewise $[(x + 1)^3] = [(x + 1)^2 + 1]$ and $[(x + 1)^4] = [(x + 1)^2 + (x + 1) + 1]$. Thus

$$\begin{aligned}
&\varphi([a_1 + b_1y + c_1y^2])\varphi([a_2 + b_2y + c_2y^2]) \\
&= [a_1 + b_1(x + 1) + c_1(x + 1)^2])([a_2 + b_2(x + 1) + c_2(x + 1)^2] \\
&= [a_1a_2 + (a_1b_2 + a_2b_1)(x + 1) + (b_1b_2 + a_1c_2 + a_2c_1)(x + 1)^2 \\
&\quad + (b_1c_2 + b_2c_1)(x + 1)^3 + c_1c_2(x + 1)^4] \\
&= [a_1a_2 + (a_1b_2 + a_2b_1)(x + 1) + (b_1b_2 + a_1c_2 + a_2c_1)(x + 1)^2 \\
&\quad + (b_1c_2 + b_2c_1)((x + 1)^2 + 1) + c_1c_2((x + 1)^2 + (x + 1) + 1)] \\
&= \varphi\big([a_1a_2 + (a_1b_2 + a_2b_1)y + (b_1b_2 + a_1c_2 + a_2c_1)y^2 \\
&\quad + (b_1c_2 + b_2c_1)(y^2 + 1) + c_1c_2(y^2 + y + 1)]\big) \\
&= \varphi\big([a_1a_2 + (a_1b_2 + a_2b_1)y + (b_1b_2 + a_1c_2 + a_2c_1)y^2 + (b_1c_2 + b_2c_1)y^3 + c_1c_2y^4]\big) \\
&= \varphi\big([a_1 + b_1y + c_1y^2][a_2 + b_2y + c_2y^2]\big)
\end{aligned}$$

So we see that φ is an isomorphism between these two fields of order 8.

Exercises

1. Construct the multiplication table for $\mathbb{G} = \mathbb{Z}_2[y]/(y^3 + y^2 + 1)$.

2. Construct the multiplication table for $\mathbb{F} = \mathbb{Z}_3[x]/(x^2 + x - 1)$.

3. (a) Factor $X^9 - X$ in $\mathbb{Z}_3[X]$.
(b) Factor $X^9 - X$ in $\mathbb{Q}[x]/(x^5 + 7x^2 - 7)$.

4. Show that $\mathbb{F} = \mathbb{Z}_3[x]/(x^2 + x - 1)$ is isomorphic to $\mathbb{G} = \mathbb{Z}_3[y]/(y^2 + 1)$.

5. (a) Show that $x^2 + 1$ and $x^2 + x + 4$ are irreducible in $\mathbb{Z}_{11}[x]$.
(b) Factor $X^2 + X + 4$ in $\mathbb{F} = \mathbb{Z}_{11}[x]/(x^2 + 1)$.
(c) Construct an explicit isomorphism from $\mathbb{G} = \mathbb{Z}_{11}[x]/(x^2 + x + 4)$ onto the field $\mathbb{F}$.

6. (a) Find all irreducible quadratics in $\mathbb{Z}_2[x]$.
(b) Construct a 4-element field.
(c)★ Show that this list of four matrices with coefficients in $\mathbb{Z}_2$

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

form a field under the usual addition and multiplication of matrices, modulo 2.
(d)★ Find an isomorphism between the fields that you constructed in parts (b) and (c).

7.3. Fermat's Little Theorem for Finite Fields

In this section, we will show that certain results about modular arithmetic for $\mathbb{Z}_p$ are valid for all finite fields. Moreover, the proofs in many cases are almost unchanged from the integer case. This will lead to strong structural results for finite fields.

7.3.1. Proposition. *Let p be prime, and let $q(x)$ be an irreducible polynomial of degree d in $\mathbb{Z}_p[x]$. Then the field $\mathbb{Z}_p[x]/(q)$ has cardinality p^d.*

Proof. This is just the observation that each $[a]$ agrees with $[r]$ where r is its remainder on dividing a by q. This remainder has degree at most $d - 1$. Conversely, two distinct polynomials r_1 and r_2 of degree at most $d-1$ must represent different equivalence classes. This is because $r_1 \equiv r_2 \pmod{q}$ if and only if q divides $r_1 - r_2$, a polynomial of degree at most $d - 1$. Since q has larger degree, this can happen only when $r_1 - r_2 = 0$. So $r_1 = r_2$.

It remains to count the number of polynomials of degree at most $d - 1$ in $\mathbb{Z}_p[x]$. They can be written as $a_0 + a_1x \ldots + a_{d-1}x^{d-1}$ where each a_i is an arbitrary element of $\mathbb{Z}_p$. There are p choices for each coefficient a_i. Hence there are p^d choices for the different equivalence classes. ■

In order to show that all finite fields are of this type, we must develop various properties of finite fields. The first result is the analogue of Fermat's little theorem.

7.3.2. Theorem. *Let $\mathbb{F}$ be a finite field of cardinality n. Then $a^{n-1} = 1$ for every $a \neq 0$ in $\mathbb{F}$.*

Proof. The proof is the same as in $\mathbb{Z}_p$. Define a map $f : \mathbb{F} \to \mathbb{F}$ by $f(x) = ax$. This map is one-to-one. To see this, notice that if $f(x) = f(y)$, then

$$0 = f(x) - f(y) = a(x - y).$$

Since $a \neq 0$ and $\mathbb{F}$ has no zero divisors, it follows that $x = y$. Also, $f(0) = 0$. Thus f maps $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ into itself. A one-to-one function of a finite set into itself must also be onto. So multiplication by a merely permutes the units. Therefore,

$$\prod_{x \in \mathbb{F}^*} x = \prod_{x \in \mathbb{F}^*} ax = a^{n-1} \prod_{x \in \mathbb{F}^*} x.$$

Dividing by the product of the units, we get $a^{n-1} = 1$. ■

7.3.3. Corollary. *Let $\mathbb{F}$ be a finite field of cardinality n. Then one can factor the polynomial $X^n - X$ in $\mathbb{F}[X]$ as $X^n - X = \prod_{a \in \mathbb{F}} (X - a)$.*

Proof. By the previous theorem, every $a \in \mathbb{F}^*$ is a root of $X^{n-1} - 1$. Thus every element of $\mathbb{F}$ is a root of $X^n - X$. This provides n roots for this polynomial of degree n. Hence it is a scalar multiple of $\prod_{a \in \mathbb{F}} (X - a)$. Since the leading coefficient of both polynomials is 1, they are equal. ■

7.3.4. Corollary. *Let q be an irreducible polynomial of degree d in $\mathbb{Z}_p[x]$, and form the field $\mathbb{F} = \mathbb{Z}_p[x]/(q)$. Then q divides $x^{p^d} - x$ in $\mathbb{Z}_p[x]$; and $q(X)$ factors into linear terms in $\mathbb{F}[X]$.*

Proof. Let $a = [x]$ be the known root of q in $\mathbb{F}$. Thinking of a as an algebraic element over $\mathbb{Z}_p$, we see that q must be the minimal polynomial of a in $\mathbb{Z}_p[X]$ because it is irreducible. Now by Theorem 7.3.2 for $\mathbb{F}$ and Proposition 7.3.1, we see that a is a root of $X^{p^d} - X$. So by Theorem 6.6.2, it follows that $q(X)$ divides $X^{p^d} - X$ in $\mathbb{Z}_p[X]$, say $X^{p^d} - X = q(X)r(X)$.

By the previous corollary, $X^{p^d} - X$ factors into a product of linear terms. By unique factorization into irreducible polynomials in $\mathbb{F}[X]$, it follows that $q(X)$ factors into a product of d linear terms in $\mathbb{F}[X]$. ■

Exercises

1. Find the analogue of Wilson's Theorem for the product of all the units of any finite field.

2. Factor $x^{16} - x$ into irreducibles in $\mathbb{Z}_2[x]$.

3. Let R be a finite integral domain. Prove that R is a field.
HINT: Take $a \neq 0$ in R and find $0 \leq m < n$ such that $a^m = a^n$.

4. Let p be an odd prime, and let $q(x) = x^{p-1} - 1 - \prod_{k=1}^{p-1}(x-k)$ in $\mathbb{Z}_p[x]$. Show that $\deg q < p-1$ but q has at least $p-1$ roots. Hence deduce Wilson's theorem for $\mathbb{Z}_p$.

7.4. Characteristic

Now it is possible to count the number of elements in a finite field. The prime integer p in the following theorem is called the **characteristic** of the field. This is the smallest integer p such that the sum of p ones in $\mathbb{F}$ equals 0. If such a sum is never 0, say that the field has characteristic zero. Examples of fields of characteristic zero are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

7.4.1. Theorem. *Let $\mathbb{F}$ be a finite field. Then*

(1) *There is a prime p so that $pa = 0$ for every $a \in \mathbb{F}$.*
(2) *$\mathbb{F}$ contains a copy of $\mathbb{Z}_p$.*
(3) *There is an integer d so that $|\mathbb{F}| = p^d$.*

Proof. First consider the elements of $\mathbb{F}$ given by 0, 1, $2 = 1+1$, $3 = 1+1+1$, and so on. This is an infinite list, and since these are all elements of the finite set $\mathbb{F}$, the list must repeat itself. So there are sums

$$k = \underbrace{1 + \ldots + 1}_{k \text{ ones}} = \underbrace{1 + \ldots + 1}_{m \text{ ones}} = m.$$

subtracting yields

$$0 = m - k = \underbrace{1 + \ldots + 1}_{m-k \text{ ones}}.$$

Let p be the smallest positive integer such that the sum of p ones equals 0. It must be shown that p is prime. If it isn't prime, factor $p = jk$ where $1 < j, k < p$. Then

$$0 = \underbrace{1 + \ldots + 1}_{p \text{ ones}} = (\underbrace{1 + \ldots + 1}_{j \text{ ones}})(\underbrace{1 + \ldots + 1}_{k \text{ ones}}) = jk.$$

Neither of these terms is 0, so $\mathbb{F}$ contains zero divisors, which is absurd. Therefore p is prime. Now for any element $a \in \mathbb{F}$,

$$pa = \underbrace{a + \ldots + a}_{p\ a\text{'s}} = a(\underbrace{1 + \ldots + 1}_{p \text{ ones}}) = a(0) = 0.$$

Let $S = \{0, 1, \ldots, p-1\}$ be the set of all possible sums of ones in $\mathbb{F}$. Notice that this set is closed under addition and multiplication (because the product of two sums of ones is a sum of ones). Moreover, by the paragraph above, addition is calculated mod p. Clearly then, multiplication is also calculated mod p. So S is a copy of $\mathbb{Z}_p$ in $\mathbb{F}$. From now on, we will write an integer n to mean $n \pmod p$ as an element of $\mathbb{F}$.

The next problem is to find a way to represent the elements of $\mathbb{F}$ which will allow us to count them. The idea is to find a minimal list $a_1 = 1$, a_2, ..., a_d in $\mathbb{F}$ so that every $a \in \mathbb{F}$ can be expressed as a sum

$$\sum_{i=1}^{d} n_i a_i \qquad n_i \in \mathbb{Z}_p.$$

This is done recursively. If $\mathbb{F}$ is larger than $\mathbb{Z}_p$, choose some element $a_2 \in \mathbb{F}$ not in $\mathbb{Z}_p$. Then if $\{n_1 + n_2 a_2 : n_i \in \mathbb{Z}_p\}$ is not all of $\mathbb{F}$, choose $a_3 \in \mathbb{F}$ not in this set. Repeat this until a set $a_1 = 1$, a_2, ..., a_d is chosen so that

- $a_j \notin \{\sum_{i=1}^{j-1} n_i a_i : n_i \in \mathbb{Z}_p\}$
- Every $a \in \mathbb{F}$ can be expressed as $\sum_{i=1}^{d} n_i a_i$ for some $n_i \in \mathbb{Z}_p$.

The important point of this representation is that every $a \in \mathbb{F}$ can be represented as such a sum *in exactly one way.* If this were not the case, there would be two different sums with the same total:

$$\sum_{i=1}^{d} m_i a_i = \sum_{i=1}^{d} n_i a_i.$$

Subtracting yields

$$\sum_{i=1}^{d} (m_i - n_i) a_i = 0.$$

It suffices to show that if $\sum_{i=1}^{d} k_i a_i = 0$, then all the coefficients k_i are 0. If this were not so, let i_0 be the largest integer so that $k_{i_0} \neq 0$. Then rearranging the equation and dividing by k_{i_0} yields

$$a_{i_0} = \sum_{i=1}^{i_0 - 1} -k_{i_0}^{-1} k_i a_i.$$

This contradicts the fact that no a_j can be written as a combination of the earlier a_i's.

It follows that each coefficient n_i can be any element of $\mathbb{Z}_p$. Since different choices yield different sums, there are p^d such sums. Thus $\mathbb{F}$ has p^d elements. ■

It is worth remarking that the last part of this proof is not really a mysterious one. If the reader is familiar with vector spaces and linear algebra, then the proof may be shortened considerably. Once $\mathbb{F}$ contains a copy of the field $\mathbb{Z}_p$, it follows that $\mathbb{F}$ is a vector space over $\mathbb{Z}_p$. If d is the dimension of $\mathbb{F}$, then $|\mathbb{F}| = p^d$. Indeed, the set $a_1, \ldots, a_d$ is a basis for $\mathbb{F}$ as a vector space over $\mathbb{Z}_p$.

Exercises

1. Show that if $\mathbb{F}$ is a field of characteristic 0, then $\mathbb{F}$ contains a copy of the rational numbers.

2. (a) For the field $\mathbb{Z}_3[X]/(x^4+x^3-1)$, show that the set $\{1,[x],[x^2],[x^3]\}$ serves the role of $\{a_1,a_2,a_3,a_4\}$ in the proof of Theorem 7.4.1.
(b)★ If you know some linear algebra, find the matrix for the linear transformation $T[p]=[xp]$ with respect to this basis.

3. Let $\mathbb{F}$ be a field of characteristic $p>0$.
(a) Prove that $(x+a)^p = x^p + a^p$ for $a \in \mathbb{F}$.
HINT: use the binomial theorem. What is $\binom{p}{k} \pmod p$?
(b) Deduce that if $a,b \in \mathbb{F}$, then $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ for every $k \geq 1$.

4. Let $\mathbb{F}$ be a field of characteristic p.
(a) Prove that $\binom{p-1}{k} \equiv (-1)^k \pmod p$ for $0 \leq k \leq p-1$.
(b) Hence show that if $a,b \in \mathbb{F}$, then $(a-b)^{p-1} = \sum_{k=0}^{p-1} a^k b^{p-1-k}$.

5. Suppose that $\mathbb{G} \subsetneq \mathbb{F}$ is a strict inclusion of finite fields of characteristic $p>0$. Let $|\mathbb{G}| = p^d$ and $|\mathbb{F}| = p^e$. Modify the proof of Theorem 7.4.1 (3) to show that $d|e$.

7.5. Algebraic Elements

If a is an element of a field $\mathbb{F}$ of cardinality p^d, then by Fermat's Little Theorem, a is a root of the polynomial $X^{p^d} - X$ in $\mathbb{Z}_p[X]$. Thus there is an irreducible factor $q(X)$ of $X^{p^d} - X$ such that $q(a) = 0$. This is the minimal polynomial of a, which is **algebraic** over $\mathbb{Z}_p$. Theorem 6.6.2 is valid for $\mathbb{Z}_p$ as well as $\mathbb{Q}$, and one can use the same proof verbatim replacing $\mathbb{Q}$ by $\mathbb{Z}_p$. Thus we conclude that if $r(a) = 0$, then $q|r$. We state this for future reference.

7.5.1. Proposition. *If a is an element of a field $\mathbb{F}$ of cardinality p^d, then a has a minimal polynomial $q \in \mathbb{Z}_p[X]$. The polynomial q is a factor of $X^{p^d} - X$. If $r \in \mathbb{Z}_p[X]$ satisfies $r(a) = 0$, then q divides r.*

Starting with this element a in $\mathbb{F}$, consider the set $\mathbb{Z}_p[a]$ of all polynomials of a. This set is a subset of $\mathbb{F}$ which is closed under addition and multiplication because

$$r(a) + s(a) = (r+s)(a) \quad \text{and} \quad r(a)s(a) = (rs)(a)$$

for all r and s in $\mathbb{Z}_p[X]$. Say that a is a **generator** of $\mathbb{F}$ if $\mathbb{F} = \mathbb{Z}_p[a]$. The following theorem explains what this subset is.

7.5.2. Theorem. *Let a be an element of a field $\mathbb{F}$ of cardinality p^d, with minimal polynomial $q \in \mathbb{Z}_p[X]$. Then $\mathbb{Z}_p[a]$ is a field isomorphic to $\mathbb{Z}_p[X]/(q)$.*

Proof. Define a map $\varphi : \mathbb{Z}_p[X] \to \mathbb{Z}_p[a]$ by $\varphi(r) = r(a)$. We have just seen that

$$\varphi(r+s) = (r+s)(a) = r(a) + s(a) = \varphi(r) + \varphi(s)$$

and

$$\varphi(rs) = (rs)(a) = r(a)s(a) = \varphi(r)\varphi(s).$$

So φ preserves addition and multiplication.

The map φ is not one to one. Indeed, $\varphi(r) = 0$ if and only if $r(a) = 0$ which occurs if and only if $q|r$ by Proposition 7.5.1. Hence $\varphi(r_1) = \varphi(r_2)$ if and only if $q|(r_1 - r_2)$ which holds if and only if $r_1 \equiv r_2 \pmod{q}$. So we may define a map $\tilde{\varphi} : \mathbb{Z}_p[X]/(q) \to \mathbb{F}$ by

$$\tilde{\varphi}([r]) = r(a).$$

The value of $\tilde{\varphi}([r])$ is independent of choice of representative r, so $\tilde{\varphi}$ is well defined on equivalence classes mod q. Therefore this definition makes sense. Moreover, our calculation also shows that $\tilde{\varphi}$ is one to one. Both sets have cardinality p^d. Thus the map $\tilde{\varphi}$ is a bijection of $\mathbb{Z}_p[X]/(q)$ onto $\mathbb{Z}_p[a]$.

Next notice that $\tilde{\varphi}$ preserves addition and multiplication because φ does. In other words,

$$\tilde{\varphi}([r]) + \tilde{\varphi}([s]) = \varphi(r) + \varphi(s) = \varphi(r+s) = \tilde{\varphi}([r+s]).$$

and

$$\tilde{\varphi}([r])\tilde{\varphi}([s]) = \varphi(r)\varphi(s) = \varphi(rs) = \tilde{\varphi}([rs]).$$

So $\tilde{\varphi}$ is a bijection between $\mathbb{Z}_p[X]/(q)$ and $\mathbb{Z}_p[a]$ which preserves all the field operations, i.e., it is an isomorphism. ■

Since the cardinality of $\mathbb{Z}_p[a]$ is at most p^d, we obtain the following consequence.

7.5.3. Corollary. *Let a be an element of a field $\mathbb{F}$ of cardinality p^d with minimal polynomial $q \in \mathbb{Z}_p[X]$. Then $\deg q \leq d$ and $\mathbb{Z}_p[a] = \mathbb{F}$ if and only if $\deg q = d$.*

7.5.4. Example. Consider the field $\mathbb{F} = \mathbb{Z}_3[x]/(x^3 + x^2 + 2)$, and the element $a = [x^2 + x + 2]$. Compute $a^2 = [x^2 + 2x + 2]$ and $a^3 = [x^2 + x]$. So we observe that a is a root of $q(X) = X^3 + 2X + 2$. This is irreducible because it is a cubic with no roots in $\mathbb{Z}_3$. To compute a^{-1} in $\mathbb{F}$, we notice that

$$0 = a^{-1}(a^3 + 2a + 2) = a^2 + 2 - a^{-1}.$$

Thus $a^{-1} = a^2 - 1$. Now we may factor $q = (X - a)(X^2 + aX + a^{-1})$ in $\mathbb{F}[X]$. The quadratic factor will have roots

$$\frac{-a \pm \sqrt{a^2 - 4a^{-1}}}{2} = \frac{-a \pm \sqrt{a^2 - 1(a^2 - 1)}}{2} = \frac{2a \pm 2}{2} = a \pm 1.$$

So

$$q(X) = (X - a)(X - a - 1)(X - a - 2).$$

We also might notice that since $a^3 = a+1$, that a^3 has the same minimal polynomial as a. Also

$$a^9 = (a^3)^3 = (a + 1)^3 = a^3 + 3a^2 + 3a + 1 = a^3 + 1 = a + 2.$$

Hence a^9 is the third root. Finally, notice that

$$a^{27} = (a + 2)^3 = a^3 + 6a^2 + 18a + 8 = a^3 + 2 = a.$$

This is foreshadowing of a general phenomenon that we will study in the section on automorphisms.

Exercises

1. In the field $\mathbb{F} = \mathbb{Z}_2[x]/(x^4 + x^3 + 1)$, find the minimal polynomial of the element $a = [x^2 + 1]$.
HINT: compute the first four powers of a and find a linear relationship among $\{1, a, a^2, a^3, a^4\}$.

2. What is the cardinality of the subfield $\mathbb{Z}_2[b] \subset \mathbb{F}$ in the previous exercise for $b = [x^3 + x]$.

3. In the field $\mathbb{F} = \mathbb{Z}_{19}[x]/(x^2 - 2)$, show that every element of $\mathbb{F} \setminus \mathbb{Z}_{19}$ has a minimal polynomial of degree 2.

4. Use Section 7.4 Exercise 5 to show that if $a \in \mathbb{F}$ with minimal polynomial $q(x) \in \mathbb{Z}_p[x]$ and $|\mathbb{F}| = p^d$, then $\deg q$ divides d.

7.6. Finite Fields

We will see now that all finite fields of characteristic p arise from arithmetic modulo an irreducible polynomial over $\mathbb{Z}_p$. To get finer detail about the structure of $\mathbb{F}$, we will need to know about primitive roots. Recall that a **primitive root** of $\mathbb{F}$ is a unit a such that the set of powers of a, $\{a, a^2, \ldots, a^{n-1}\}$, is the full set of units $\mathbb{F}^*$. In particular, primitive roots are generators of $\mathbb{F}$.

7.6.1. Theorem. *Every finite field has a primitive root.*

Proof. Again, the proof is the same as for $\mathbb{Z}_p$. Let $n = |\mathbb{F}| = p^d$. The **order** of a unit a is defined to be the least positive integer $d = \mathrm{ord}(a)$ such

that $a^d = 1$. As in Proposition 2.10.2, it follows that if $a^k = 1 = a^\ell$, then $a^{\gcd(k,\ell)} = 1$ as well. Since $a^{n-1} = 1$, it then follows that $\mathrm{ord}(a)|n-1$ as in Corollary 2.10.3.

Following the proof of Lemma 2.10.5, let $f(d)$ count the number of elements $a \in \mathbb{F}$ with $\mathrm{ord}(a) = d$ for each d which divides $n-1$. As before, notice that $\mathrm{ord}(a)|d$ if and only if a is a root of $X^d - 1$ in $\mathbb{F}$. This polynomial has at most d roots. On the other hand,

$$X^{n-1} - 1 = (X^d - 1)(X^{n-1-d} + X^{n-1-2d} \ldots + X^d + 1)$$

has exactly $n-1$ roots by Corollary 7.3.3. The second factor has at most $n-1-d$ roots. Thus each factor must have its full complement of roots. This yields the formula

$$\sum_{e|d} f(e) = d.$$

As in the proof of Theorem 2.10.6, observe that this set of equations is also satisfied by the Euler φ function. So as in that proof, we deduce that $f(d) = \varphi(d)$ for every divisor d of $n-1$. In particular, there are $\varphi(n-1)$ elements of order $n-1$. These are the primitive roots. ■

We can use primitive roots to provide a familiar criterion for when an element of $\mathbb{F}$ is a square.

7.6.2. Proposition. *Let p be an odd prime, and let $\mathbb{F}$ be a field of cardinality p^d. An element $a \in \mathbb{F}$ is a square in $\mathbb{F}$ if and only if $a^{(p^d-1)/2} = 1$.*

Proof. Let $c = a^{(p^d-1)/2}$. Then by Fermat's little theorem for $\mathbb{F}$, $c^2 = a^{p^d-1} = 1$. Thus c is a root of $x^2 - 1 = 0$; whence $c \in \{\pm 1\}$.

Let b be a primitive root for $\mathbb{F}$. Then $b^{(p^d-1)/2} = -1$ since it is distinct from $b^{p^d-1} = 1$. If $a = b^k$ for $0 \le k < p^d - 1$, then

$$a^{(p^d-1)/2} = \left(b^{(p^d-1)/2}\right)^k = (-1)^k.$$

This equals 1 if and only if k is even.

If $a = d^2$ for some $d \in \mathbb{F}$ and $d = b^l$ for $0 \le l < p^d - 1$, then $a = b^{2l}$. So $k \equiv 2l \pmod{p^d - 1}$. Since $2l$ and $p^d - 1$ are both even, this forces k to be even. Conversely, if $k = 2l$, then $a = (b^l)^2$ is a square. ■

Now we have the necessary tools to prove the main theorem about finite fields.

7.6.3. Theorem. *Let $\mathbb{F}$ be a finite field of cardinality p^n. There is an irreducible polynomial $q \in \mathbb{Z}_p[x]$ of degree n so that $\mathbb{F}$ is isomorphic to $\mathbb{Z}_p[x]/(q)$. Moreover, $X^{p^n} - X = \prod_{a\in\mathbb{F}}(X-a)$ factors into linear terms with p^d distinct roots.*

Proof. Let a be a primitive root of $\mathbb{F}$. Let q be the minimal polynomial of a. The subfield $\mathbb{Z}_p[a]$ contains a^k for $0 \leq k \leq p^d - 1$. As this is a list of all the non-zero elements of $\mathbb{F}$, we obtain $\mathbb{Z}_p[a] = \mathbb{F}$. By Theorem 7.5.2, there is an isomorphism of $\mathbb{Z}_p[X]/(q)$ onto $\mathbb{F}$. Since

$$p^{\deg(q)} = |\mathbb{Z}_p[X]/(q)| = |\mathbb{F}| = p^n,$$

we see that q has degree exactly n.

By Corollary 7.3.3, $X^{p^n} - X = \prod_{a \in \mathbb{F}}(X - a)$ in $\mathbb{F}[X]$. This is degree p^n and has p^n distinct roots. ■

Since there are different irreducible factors of degree d, it is possible that there are many different finite fields of each cardinality. However, this is not the case.

7.6.4. Corollary. *There is only one field $\mathbb{F}$ of cardinality p^n up to isomorphism.*

Proof. Suppose that $\mathbb{F}$ and $\mathbb{G}$ are finite fields of cardinality p^n. By Theorem 7.6.3, there is an irreducible polynomial q of degree n so that $\mathbb{F}$ is isomorphic to $\mathbb{Z}_p[X]/(q)$. Moreover, q is a factor of $X^{p^n} - X$, so we obtain a factorization $X^{p^n} - X = q(X)r(X)$.

By Corollary 7.3.3 applied to $\mathbb{G}$, we see that $X^{p^n} - X$ factors into linear terms in $\mathbb{G}[X]$. As we have seen before, the polynomial $q(X)$ must have exactly n roots in $\mathbb{G}$. Let b be such a root. Then the minimal polynomial of b in $\mathbb{Z}_p[X]$ is q since q is irreducible. By Theorem 7.5.2, $\mathbb{Z}_p[X]/(q)$ is isomorphic to $\mathbb{Z}_p[b]$. In particular, $\mathbb{Z}_p[b]$ has p^n elements, and thus is all of $\mathbb{G}$. So $\mathbb{F}$ and $\mathbb{G}$ are isomorphic are both isomorphic to $\mathbb{Z}_p[X]/(q)$, and thus to each other. ■

Because of this corollary, there is *at most one* field of cardinality p^n for each prime p and positive integer n. We will call it $\mathbb{F}_{p^n}$. We still need to show that $\mathbb{F}_{p^n}$ always exists.

7.6.5. Corollary. *Every irreducible polynomial of degree n in $\mathbb{Z}_p[x]$ splits into a product of linear terms in $\mathbb{F}_{p^n}$.*

Proof. This is an immediate corollary of Corollary 7.3.4 and the uniqueness of $\mathbb{F}_{p^n}$ established above. ■

7.6.6. Example. Consider $p(x) = x^4 + x^2 + x + 1$ in $\mathbb{Z}_3[x]$. This is irreducible. To see this, first notice that it has no roots in $\mathbb{Z}_3$. So if it factors, it is into a product of two quadratics. There are only three irreducible quadratics in $\mathbb{Z}_3[x]$, namely $x^2 + 1$, $x^2 - x - 1$ and $x^2 + x - 1$. None of these divide p, so p is irreducible. Form the field $\mathbb{F} = \mathbb{Z}_3[x]/(p)$ with 81 elements.

To find a primitive root, we require an element of order 80. As for prime integers, it suffices to show that $\text{ord}(a)$ is not a proper divisor of $80 = 2^4 5$. Thus an element a such that $a^{40} \neq 1$ and $a^{16} \neq 1$ must be a primitive root. Using computer software, we compute $[x]^{40} = 1$. A second try is $[x+1]^{40} = -1$ and $[x+1]^{16} = [x^3 - 1]$. Thus $[x+1]$ is a primitive root. Going back to the element $[x]$, we compute $[x]^{20} = [-x^3 - x^2 - x + 1]$ and $[x]^8 = [x^3 + x^2 - x]$. So $\text{ord}([x]) = 40$.

Exercises

1. Check by division that $p(x)$ in Example 7.6.6 is not divisible by any irreducible quadratic polynomial, as claimed.

2. (a) Factor $X^{16} - X$ into irreducibles in $\mathbb{Z}_2[X]$.
(b) Show that $X^3 + X + 1$ is irreducible over $\mathbb{F} = \mathbb{Z}_2[x]/(p(x))$ where $p(x) = x^4 + x^3 + x^2 + x + 1$.

3. Show that for any polynomial $q \in \mathbb{Z}_p[x]$ (where p is prime), the polynomial $q^{p^d} - q$ is divisible by $x^{p^d} - x$.
HINT: consider its roots in $\mathbb{F}_{p^d}$.

4. (a) Find $\text{ord}([x])$ in $\mathbb{F} = \mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$. Notice that $[x]$ is a generator of $\mathbb{F}$ but not a primitive root.
(b) Find a primitive root for $\mathbb{F}$.
(c) Factor $X^4 + X^3 + 1$ in $\mathbb{F}[X]$.

5. If $p \neq 3$ is prime, find a criterion for $a \in \mathbb{F}_{p^n}$ to be a perfect cube.

7.7. Automorphisms of $\mathbb{F}_{p^d}$

In the study of fields, the set of isomorphisms of the field onto itself (which are called **automorphisms**) is very important. It is a crucial idea of Galois theory. Galois theory can be used to explain why certain polynomials of degree at least 5 cannot be solved by repeated kth roots, $k \geq 2$. It is also used to show that certain angles cannot be trisected by a procedure using only a straight-edge and a compass. In the case of finite fields, we may analyze these automorphisms more concretely. The key is the following observation showing that there is a special automorphism called the **Frobenius automorphism** for each finite field.

7.7.1. Lemma. *Let $\mathbb{F}_{p^d}$ be a finite field. The map $\varphi : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$ given by*

$$\varphi(a) = a^p$$

is an isomorphism. Moreover, $\varphi(a) = a$ if and only if $a \in \mathbb{Z}_p$.

Proof. We see $\varphi(0) = 0$ and $\varphi(1) = 1$. Also,

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b).$$

So φ is multiplicative. The key is that it is also additive. Note that if $1 \leq i < p$, then $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$ is a multiple of p because p divides the numerator but not the denominator. Thus because computations in $\mathbb{F}$ are done modulo p,

$$\begin{aligned}\varphi(a+b) = (a+b)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \\ &= a^p + b^p = \varphi(a) + \varphi(b).\end{aligned}$$

Hence we see that φ preserves all the field operations. Next let us check that φ is a bijection. If

$$0 = \varphi(a) - \varphi(b) = \varphi(a-b) = (a-b)^p,$$

then it follows that $a - b = 0$ or $a = b$. So φ is a one-to-one map of $\mathbb{F}$ into itself. As $\mathbb{F}$ is finite, it is also onto. Hence φ is a bijection. Therefore it is an automorphism.

Finally, notice that $\varphi(a) = a$ if and only if a is a root of $X^p - X$. By Fermat's little theorem, every element of $\mathbb{Z}_p$ is a root. This accounts for p roots of this polynomial of degree p. Hence there are no others. ■

7.7.2. Example. Consider the field of 8 elements $\mathbb{F}_8$. The Frobenius automorphism is $\varphi(a) = a^2$. So $\varphi^2(a) = \varphi(\varphi(a)) = a^4$ is also an automorphism of $\mathbb{F}_8$. Similarly, $\varphi^3(a) = a^8$ is an automorphism. However, by Fermat's little theorem for finite fields, $a^8 = a$ for every $a \in \mathbb{F}$. So φ^3 is the identity map. Using the multiplication table 7.2.1, we can construct the following table.

a	$\varphi(a)$	$\varphi^2(a)$	$\varphi^3(a)$
0	0	0	0
1	1	1	1
x	x^2	x^2+x	x
$x+1$	x^2+1	x^2+x+1	$x+1$
x^2	x^2+x	x	x^2
x^2+1	x^2+x+1	$x+1$	x^2+1
x^2+x	x	x^2	x^2+x
x^2+x+1	$x+1$	x^2+1	x^2+x+1

FIGURE 7.7.1. Automorphisms of $\mathbb{F}_8$

Recall that we showed that in $\mathbb{F}_8[X]$, we can factor

$$X^3 + X + 1 = (X - x)(X - x^2)(X - (x^2 + x)).$$

Observe that x, $\varphi(x) = x^2$ and $\varphi(x^2) = x^2 + x$ are the three roots of this polynomial. Also $\varphi(x^2 + x) = x$; so φ just permutes the roots.

This demonstrates a useful property of automorphisms of $\mathbb{F}$ for the purpose of studying polynomials in $\mathbb{Z}_p[X]$. Every automorphism of $\mathbb{F}$ must permute the roots of these polynomials in $\mathbb{Z}_p[X]$.

7.7.3. Lemma. *Let ψ be an automorphism of $\mathbb{F}_{p^d}$. Then $\psi(a) = a$ for all $a \in \mathbb{Z}_p$. If $q \in \mathbb{Z}_p[X]$ and $a \in \mathbb{F}_{p^d}$ is a root of q, then $\psi(a)$ is also a root of q.*

Proof. First, since $\psi(1) = 1$, we have

$$\begin{aligned}\psi(k) &= \psi(\underbrace{1 + \ldots + 1}_{k \text{ terms}}) \\ &= \underbrace{\psi(1) + \ldots + \psi(1)}_{k \text{ terms}} \\ &= \underbrace{1 + \ldots + 1}_{k \text{ terms}} = k.\end{aligned}$$

This shows that ψ is the identity on $\mathbb{Z}_p$.

Now let $q(X) = q_0 + q_1 X + \ldots + q_n X^n$ be a polynomial with coefficients $q_i \in \mathbb{Z}_p$. If a is a root, then

$$\begin{aligned}0 = \psi(q(a)) &= \sum_{i=0}^{n} \psi(q_i)\psi(a^i) \\ &= \sum_{i=0}^{n} q_i \psi(a)^i = q(\psi(a)).\end{aligned}$$

So $\psi(a)$ is also a root. Indeed, applying ψ to all the roots of q yields a permutation of the roots. ■

7.7.4. Corollary. *Let a be a primitive root of $\mathbb{F}_{p^d}$, and let $q \in \mathbb{Z}_p[X]$ be its minimal polynomial. Then q has d distinct roots: $\varphi^k(a) = a^{p^k}$ for $0 \le k \le d-1$, where φ is the Frobenius automorphism.*

Proof. By the previous lemma, since a is a root of q, then so are

$$a_1 = \varphi(a) = a^p,\ a_2 = \varphi(a_1) = \varphi^2(a) = a^{p^2},\ a_3 = \varphi(a_2) = a^{p^3},$$

and so on. Indeed, each $a_k = \varphi^k(a) = a^{p^k}$ must be a root of q for all $k \ge 0$. For $0 \le k \le d-1$, these are all different roots because a is a primitive root. This accounts for all d roots of q. Of course, by Fermat's little theorem for finite fields, $\varphi^d(a) = a^{p^d} = a$. So the sequence starts repeating itself at that point. ■

7.7.5. Lemma. *Let $\mathbb{F}_{p^d}$ be a finite field, and let a be a generator of $\mathbb{F}_{p^d}$. If ψ_1 and ψ_2 are automorphisms of $\mathbb{F}$ such that $\psi_1(a) = \psi_2(a)$, then $\psi_1 = \psi_2$.*

Proof. Since ψ_i are isomorphisms, it follows that

$$\psi_1(r(a)) = r(\psi_1(a)) = r(\psi_2(a)) = \psi_2(r(a))$$

for every polynomial $r \in \mathbb{Z}_p[X]$. Since a is a generator, this accounts for every non-zero element of $\mathbb{F}$. So $\psi_1 = \psi_2$. ■

This brings us to the main theorem of this section.

7.7.6. Theorem. *Let $\mathbb{F}_{p^d}$ be a finite field, and let φ be the Frobenius automorphism. Then d is the smallest positive integer k such that $\varphi^k = id$. Moreover, the set of all automorphisms of $\mathbb{F}_{p^d}$ is given by*

$$\{id, \varphi, \varphi^2, \ldots, \varphi^{d-1}\}.$$

Proof. Notice that $\varphi^k(a) = a^{p^k}$. Hence the fixed point set

$$\{a \in \mathbb{F}_{p^d} : \varphi^k(a) = a\}$$

consists of the roots of the polynomial $X^{p^k} - X$. For $k < d$, this is a proper subset of $\mathbb{F}_{p^d}$ because the polynomial has at most p^k roots. So $\varphi^k \neq id$. But every element of $\mathbb{F}_{p^d}$ is a root of $X^{p^d} - X$ by Fermat's little theorem for finite fields. Thus $\varphi^d = id$.

Let ψ be any automorphism of $\mathbb{F}_{p^d}$. Fix a primitive root a in $\mathbb{F}_{p^d}$, and let q be its minimal polynomial in $\mathbb{Z}_p[X]$. By Lemma 7.7.3, $\psi(a)$ is another root of q. And by Corollary 7.7.4, there is an integer k so that $\psi(a) = \varphi^k(a)$. By Lemma 7.7.5, $\psi = \varphi^k$. Therefore every automorphism of $\mathbb{F}_{p^d}$ is a power of the Frobenius automorphism. ■

Exercises

1. Let $\mathbb{F} = \mathbb{Z}_5[x]/(x^4 + x^2 + x + 1)$. Show that $q(X) = X^4 + X^2 + X + 1$ factors as

$$q(X) = (X - x)(X - x^5)(X - x^{25})(X - x^{125}).$$

2. With $\mathbb{F}$ as above, use the fact that $x^2 + 1$ is a root of the irreducible polynomial $X^4 - 2X^3 - 2X^2 + 2X + 2$ to find the other roots.

3. Show that every $a \in \mathbb{F}_{p^n}$ has a unique pth root.

4. Let p be prime and $n \in \mathbb{N}$. Show that n divides the Euler number $\varphi(p^n - 1)$.
HINT: this is the number of primitive roots. Show that they split into disjoint subsets $S_a = \{\varphi^k(a) : 0 \leq k < n\}$ of size n for primitive roots a.

5. (a) For any divisor d of n, show that the roots of $X^{p^d} - X$ in $\mathbb{F}_{p^n}$ form a subfield isomorphic to $\mathbb{F}_{p^d}$.
HINT: Use the fact that φ^d is an automorphism to show that this set of roots forms a field.
(b) Deduce that this is the unique subfield of cardinality p^d.
(c) Show that every automorphism of $\mathbb{F}_{p^n}$ maps this subfield onto itself.

6. If $a \in \mathbb{F}_{p^n}^*$, its **conjugates** are $\{\varphi^k(a) : 0 \le k < n\} = \{a = a_1, a_2, \ldots, a_d\}$. Let q be the minimal polynomial for a.
(a) Show that the the conjugates of a are roots of q.
(b) Show that the polynomial $p(x) = \prod_{I=1}^{d}(x - a_i)$ has coefficients which are fixed by φ.
(c) Deduce that $p = q$. So the roots of q are exactly the conjugates of a.
(d) Show that $d|n$.
HINT: the smallest $e > 0$ such that $\varphi^e(a) = a$ divides n.

7. Define the **trace** on $\mathbb{F}_{p^n}$ by $\mathrm{Tr}(a) = \sum_{k=0}^{n-1} \varphi^k(a)$.
(a) Show that $\mathrm{Tr}(a) \in \mathbb{F}_p$.
(b) Show that $\mathrm{Tr}(a + b) = \mathrm{Tr}(a) + \mathrm{Tr}(b)$ for $a, b \in \mathbb{F}_{p^n}$.
(c) Show that $\mathrm{Tr}(\beta a) = \beta\,\mathrm{Tr}(a)$ for $\beta \in \mathbb{F}_p$ and $a \in \mathbb{F}_{p^n}$.
(d) Show that $\mathrm{Tr}(\beta) = n\beta$ for $\beta \in \mathbb{F}_p$.
(e) Show that $\mathrm{Tr}(a^p) = \mathrm{Tr}(a)$ for $a \in \mathbb{F}_{p^n}$.

7.8. Irreducible polynomials of all degrees

We have made the implicit assumption in the preceding discusion that irreducible polynomials exist in abundance. In this section, we will show that there are irreducible polynomials in $\mathbb{Z}_p[X]$ of every degree for every prime p. First let us take note of something we already know.

7.8.1. Lemma. *Let $q \in \mathbb{Z}_p[X]$ be an irreducible polynomial of degree d. Then q is a factor of $X^{p^d} - X$.*

Proof. Form the field $\mathbb{Z}_p[X]/(q)$. This has p^d elements, and the element $[x]$ is a root of q. Since q is irreducible, it is the minimal polynomial of $[x]$. By Fermat's little theorem, $[x]$ is a root of $X^{p^d} - X$. Therefore, q divides $X^{p^d} - X$. ■

A converse of sorts requires some more sophisticated argument. First we need an elementary, yet rather clever, calculation.

7.8.2. Lemma. $\gcd(X^m - 1, X^n - 1) = X^d - 1$ *where* $d = \gcd(m, n)$.

Proof. If $m = dk$, then

$$X^m - 1 = (X^d - 1)(1 + X^d + X^{2d} + \ldots + X^{(k-1)d}).$$

Thus $X^d - 1$ divides both $X^m - 1$ and $X^n - 1$. By the Euclidean algorithm, there are positive integers s and t so that $d = ms - nt$. So if we define

$$S(X) = 1 + X^m + X^{2m} + \ldots + X^{(s-1)m}$$
$$T(X) = (1 + X^n + X^{2n} + \ldots + X^{(t-1)n})X^d.$$

Then

$$(X^m - 1)S(X) - (X^n - 1)T(X) = (X^{ms} - 1) - (X^{nt} - 1)X^d = X^d - 1.$$

So any common divisor of $X^m - 1$ and $X^n - 1$ divides $X^d - 1$. Thus the gcd of $X^m - 1$ and $X^n - 1$ equals $X^d - 1$. ■

7.8.3. Corollary. $\gcd(p^m - 1, p^n - 1) = p^d - 1$ *where* $d = \gcd(m, n)$.

Proof. Substituting p for X shows that $p^d - 1$ divides both $p^m - 1$ and $p^n - 1$. The proof of the previous lemma shows that $\gcd(p^m - 1, p^n - 1)$ divides

$$(p^m - 1)S(p) - (p^n - 1)T(p) = p^d - 1.$$

Hence $\gcd(p^m - 1, p^n - 1) = p^d - 1$. ■

7.8.4. Lemma. *Let* $q \in \mathbb{Z}_p[X]$ *be an irreducible polynomial of degree* d. *Then* q *is a factor of* $X^{p^n} - X$ *if and only if* $d|n$.

Proof. The case $q = X$ is trivial, so suppose that $q \neq X$.

Suppose that $d|n$. Then by Lemma 7.8.1, we have $q|X^{p^d-1} - 1$. By Corollary 7.8.3, $p^d - 1$ divides $p^n - 1$. Hence by Lemma 7.8.2, $X^{p^d-1} - 1$ divides $X^{p^n-1} - 1$. So q divides $X^{p^d} - X$ which divides $X^{p^n} - X$.

Conversely, suppose that q divides $X^{p^n} - X$. Since $X^{p^n} - X$ factors into linear terms in $\mathbb{F}_{p^n}$, so does q. Let $a \in \mathbb{F}_{p^n}$ be a root of q. Since q is irreducible, this is the minimal polynomial of a. Hence $\mathbb{Z}_p[a]$ is isomorphic to $\mathbb{Z}_p[x]/(q)$, which has cardinality p^d. By Corollary 7.3.3 ,

$$\prod_{b \in \mathbb{Z}_p[a]} X - b = X^{p^d} - X.$$

This divides $X^{p^n} - X$ in $\mathbb{F}_{p^n}[X]$. Because both have coefficients in $\mathbb{Z}_p$, the quotient also lies in $\mathbb{Z}_p[X]$. So $X^{p^d-1} - 1$ divides $X^{p^n-1} - 1$. By Lemma 7.8.2, $p^d - 1$ divides $p^n - 1$. And by Corollary 7.8.3, d divides n. ■

Our next goal is to show that if $q \in \mathbb{Z}_p[X]$ is an irreducible polynomial of degree d and $d|n$, then q^2 does not divide $X^{p^n} - X$. To prove this, we need a method to identify repeated roots. The key tool we use is the formal derivative.

7.8.5. Definition. Let $\mathbb{F}$ any field and let $q(x) = \sum_{i=0}^{d} q_i x^i$ be an element of $\mathbb{F}[x]$. Then, its **formal derivative** is given by

$$q'(x) = \sum_{i=1}^{d} i q_i x^{i-1}.$$

7.8.6. Lemma. *For a polynomial $q \in \mathbb{F}[X]$, all irreducible factors of q are simple if and only if $\gcd(q, q') = 1$. Moreover, if there are repeated roots, this gcd provides a proper factor except when $\mathbb{F}$ has characteristic p and q is a perfect p-th power. In either case, this yields a factorization of q.*

Proof. In Exercise 3, the reader will verify the product rule

$$(qr)' = q'r + qr'.$$

If q has a repeated factor u, then we can write $q = u^2 v$ for some $v \in \mathbb{F}[X]$. Calculate

$$q' = (u^2 v)' = 2uu'v + u^2 v' = u(2u' + uv')$$

Hence u divides $\gcd(q, q')$.

This gcd provides a proper factor of q except in the special case in which $\gcd(q, q') = q$. But since $\deg(q') < \deg(q)$, this can only occur when $q' = 0$. This can never happen over the rationals, or any field of characteristic 0. However, in a field of characteristic p, this can happen if $iq_i \equiv 0 \pmod{p}$ for every coefficient i. Clearly this means that q_i is non-zero only when $i \equiv 0 \pmod{p}$. In this case

$$q(X) = \sum_{j=0}^{m} a_j X^{jp}.$$

Let $u = \sum_{j=0}^{m} a_j X^j$. By Lemma 7.7.1 above, the p-th power of a sum is the sum of the p-th powers in any field of characteristic p. In particular, $q = u^p$. This yields a factorization of q.

Conversely, suppose that u is an irreducible factor of q which is simple, so that $q = uv$ where $v \in \mathbb{F}[X]$ satisfies $\gcd(u, v) = 1$. Then

$$q' = (uv)' = u'v + uv' \equiv u'v \pmod{u}$$

Now $u' \neq 0$ since u is irreducible (and thus is not a p-th power), and u' is of lower degree than u. So both u' and v are relatively prime to u. By the unique factorization theorem, the product $u'v$ is also relatively prime to u. Hence u is not a factor of q'.

Consequently, if q has only simple factors, it can have no factor in common with q'. Therefore $\gcd(q, q') = 1$. ∎

We can now describe the factorization of $X^{p^n} - X$ into irreducibles in $\mathbb{Z}_p[X]$.

7.8.7. Corollary. *$X^{p^n} - X$ factors in $\mathbb{Z}_p[X]$ as the product of all irreducible polynomials q of degree d as d runs over all divisors of n.*

Proof. Let $f(X) = X^{p^n} - X$. The formal derivative is

$$f'(X) = p^n X^{p^n - 1} - 1 = -1$$

and so $\gcd(f, f') = 1$. Since $f(X)$ is not a perfect p-th power, by Lemma 7.8.6, all of the irreducible factors of $f(X)$ are simple. The result now follows from Lemma 7.8.4. ■

We are finally ready to prove the main result of this section.

7.8.8. Theorem. *There are irreducible polynomials in $\mathbb{Z}_p[X]$ of degree n for every n.*

Proof. Let $r_d(X)$ denote the product of all monic irreducible polynomials of $\mathbb{Z}_p[X]$ of degree d. From Corollary 7.8.7, we obtain that

$$X^{p^n} - X = \prod_{d|n} r_d(X).$$

Therefore

$$p^n = \deg(X^{p^n} - X) = \sum_{d|n} \deg(r_d(X)).$$

We will show that r_n is non-zero by showing that the sum of the degrees of the other factors of $X^{p^n} - X$ is strictly less than p^n. Note that since r_d divides $X^{p^d} - X$, it has $\deg(r_d) \leq p^d$. Thus a crude estimate shows

$$\deg\Big(\prod_{\substack{d|n \\ d \neq n}} r_d\Big) \leq \sum_{d|n} p^d \leq \sum_{i=1}^{n-1} p^i = \frac{p^n - p}{p - 1} < p^n.$$

So r_n must have non-zero degree. ■

7.8.9. Remark. We are able to prove Theorem 7.8.8 by crudely bounding the number of irreducible polynomials of a given degree. In Exercise 7, we prove a formula giving the exact number of irreducible polynomials in $\mathbb{Z}_p[x]$ of degree n. It is actually rather large.

Here are two easy consequences of this theorem.

7.8.10. Corollary. *There is a finite field $\mathbb{F}_{p^n}$ of cardinality p^n for every prime p and integer $n \geq 1$.*

7.8.11. Corollary. *There are irreducible polynomials of every degree in $\mathbb{Z}[X]$ using only 0's and 1's as coefficients.*

Proof. Take an irreducible polynomial of degree n in $\mathbb{Z}_2[X]$. Then the corresponding polynomial in $\mathbb{Z}[X]$ is irreducible by Corollary 6.5.2. ■

7.8.12. Example. Consider the polynomial $X^{31}-1$ in $\mathbb{Z}_7[X]$. First look for the smallest integer d so that $X^{31}-1$ divides $X^{7^d-1}-1$. By Lemma 7.8.2, this occurs precisely when 31 divides 7^d-1; that is, when $7^d \equiv 1 \pmod{31}$. So we are interested in $\mathrm{ord}_{31}(7)$. By Fermat's little theorem, this is a divisor of 30. A calculation shows that

$$7^3 \equiv 2 \pmod{31} \quad \text{and} \quad 7^5 \equiv 5 \pmod{31}.$$

Therefore, $7^6 \equiv 4 \pmod{31}$, $7^{10} \equiv -6 \pmod{31}$ and $7^{15} \equiv 1 \pmod{31}$. Hence, $\mathrm{ord}_{31}(7) = 15$.

So $X^{31}-1$ divides $X^{7^{15}-1}-1$. Since 31 is prime, Lemma 7.8.2 yields that

$$\gcd(X^{31}-1, X^{7^3-1}-1) = X-1 = \gcd(X^{31}-1, X^{7^5-1}-1).$$

Consequently, it follows from Lemma 7.8.4 that $X^{31}-1$ has one linear factor, $X-1$, and no irreducible factors of degree 3 or 5. Therefore it must factor as the product of $X-1$ and two irreducible polynomials p_1, p_2 of degree 15. Symbolic computation software such as MAPLE or MATHEMATICA can find these factors easily. In particular, p_1 equals

$$X^{15}-2X^{14}+X^{13}-3X^{12}-X^{11}-3X^{10}+3x^9-2X^7-X^6+3X^5-3X^4+X^3+X^2-3X-1.$$

Consider the field $\mathbb{F} = \mathbb{Z}_7[x]/(p_1)$ of order 7^{15}. The element $[x]$ is a root of p_1, and thus is a root of $X^{31}-1$. Hence $\mathrm{ord}([x])$ divides 31. Since $[x] \neq [1]$ and 31 is prime, we find that $\mathrm{ord}([x]) = 31$. In particular, $[x]$ is not a primitive root. However, it is clearly a generator of $\mathbb{F}$.

Let us try to count the irreducible factors of $X^{7^{15}}-X$. From the theory we have developed, it factors as

$$X^{7^{15}} - X = r_1(X) r_3(X) r_5(X) r_{15}(X)$$

where $r_d(X)$ is the product of all monic irreducible factors of degree d. We also know that

$$\begin{aligned}
r_1(X) &= X^7 - X = X(X-1)(X-2)(X-3)(X+3)(X+2)(X+1) \\
r_3(X) &= (X^{7^3-1}-1)/(X^6-1) \\
r_5(X) &= (X^{7^5-1}-1)/(X^6-1) \\
r_{15}(X) &= \big((X^{7^{15}-1}-1)(X^6-1)\big)/\big((X^{7^3-1}-1)(X^{7^5-1}-1)\big).
\end{aligned}$$

So we see that there are 7 irreducible polynomials of degree 1. The degree of r_3 is $7^3-7 = 336$. So there are 112 irreducible polynomials of degree 3 over $\mathbb{Z}_7$. Similarly, the degree of r_5 is 7^5-7. So there are $(7^5-7)/5 = 3360$ irreducible polynomials of degree 5 over $\mathbb{Z}_7$. Finally, we calculate the degree of r_{15} to be $7^{15}-7^5-7^3+7$. Dividing by 15 yields the number 316504099520 irreducible polynomials of degree 15. There are $\varphi(7^{15}-1) = 1450340640000$

primitive roots of $\mathbb{F}$. These come in groups of 15 corresponding to the roots of 96689376000 of these irreducible polynomials of degree 15.

Exercises

1. Find an irreducible polynomial of degree 6 in $\mathbb{Z}_2[x]$.

2. How many irreducible monic polynomials of degree 6 are there in $\mathbb{Z}_2[x]$. How many of these have roots which are primitive roots in $\mathbb{F}_{64}$?

3. Verify the product rule for the formal derivative of polynomials in any field.

4. Show that the only subfields of $\mathbb{F}_{p^n}$ are the fields $\mathbb{F}_{p^d}$ for $d|n$.
HINT: combine Corollary 7.8.7 and Section 7.7 Exercise 5.

5. Show that the fixed point set of φ^k on $\mathbb{F}_{p^d}$ is the subfield $\mathbb{F}_{p^e}$ where $e = \gcd(k, d)$.

6. In this exercise, we prove the **Möbius inversion formula**. Let $\mu\colon \mathbb{Z}^+ \to \mathbb{Z}$ be defined as follows. Let $\mu(1) = 1$, $\mu(n) = 0$ if n is not square-free, and otherwise $\mu(n) = (-1)^k$, where n is a product of k distinct primes.

(a) Prove $\sum_{d|n} \mu(d)$ is 1 if $n = 1$, and 0 otherwise.
(b) For any functions $F, G : \mathbb{Z}^+ \to \mathbb{Z}$, let

$$(F * G)(n) = \sum_{d|n} F(d)G(\tfrac{n}{d}).$$

Prove $*$ is an associative commutative binary operation on functions.
(c) Find the function H which the identity for $*$.
(d) Suppose $f : \mathbb{Z}^+ \to \mathbb{Z}$ and $g : \mathbb{Z}^+ \to \mathbb{Z}$ are functions, and that

$$g(n) = \sum_{d|n} f(d).$$

Prove that

$$f(n) = \sum_{d|n} \mu(d)g(\tfrac{n}{d}).$$

7. Let p be a prime. Prove that there are

$$\frac{1}{n} \sum_{d|n} \mu(\tfrac{n}{d})p^d$$

monic irreducible degree n polynomials in $\mathbb{F}_p[x]$.

7.9. Factoring Algorithms for Polynomials

In this section, we take a brief look at one method for factoring polynomials. It turns out that it is much easier to factor a polynomial of degree d in $\mathbb{Z}_p[x]$ than to factor a number with d digits in base p. This seems, on the surface, to be a surprising fact because the number and the polynomial have the same complexity. However, it turns out that the structure of finite fields is the key.

The first step in factoring polynomials is to reduce the problem to the case in which the polynomial q has no repeated factors, which may be done usng Lemma 7.8.6. Compute $\gcd(q, q')$ and use this to factor q. Repeat as necessary until it is factored into terms with no repeated factors.

We are now ready to study the main factoring algorithm of this section. It is the preferred method used in the symbolic computation program MAPLE. Also, it is perhaps the simplest and most effective way to factor polynomials in $\mathbb{Z}[x]$. The main idea is to factor polynomials modulo p based on the Euclidean algorithm and Lemma 7.8.4. Then Hensel's Lemma, which will be discussed in the next section, is used to increase the information about the possible integer factorizations.

Lemma 7.8.4 shows that if $q \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree d, then q divides $x^{p^d} - x$ but does not divide $x^{p^k} - x$ for $k < d$. We first compute $\gcd(q, x^p - x) = r_1$. Since $x^d - x = \prod_{a \in \mathbb{Z}_p} x - a$, this will produce a factor r_1 which we will later factor into a product of linear terms. Replace q with $q_1 = q/r_1$. Next compute $\gcd(q_1, x^{p^2} - x) = r_2$. Since r_2 has no linear factors, all of its irreducible factors will be quadratic. Set $q_2 = q_1/r_1$ and define $\gcd(q_2, x^{p^3} - x) = r_3$. Then all of the irreducible factors of r_3 have degree 3. Proceed until the degree of q is reached (although this will end sooner if factors are found). For this reason, this method is known as the **distinct degree algorithm**.

Now, these factors can be distinguished by using quadratic residues in finite fields. When $p \neq 2$, half of the non-zero elements of a finite field are perfect squares. So a polynomial t of degree at most $d - 1$ will be a square modulo r_i about half the time. When t is a square in $\mathbb{Z}[x]/(r_i)$, then by Proposition 7.6.2,

$$t^{(p^d-1)/2} \equiv 1 \pmod{r_i}.$$

And when t is not a square,

$$t^{(p^d-1)/2} \equiv -1 \pmod{r_i}.$$

So it suffices to compute

$$\gcd(r, t^{(p^d-1)/2} - 1)$$

for several random choices of t to obtain various proper factors of r.

We won't work out exactly what happens when $p = 2$. Let $f(x) = \sum_{i=1}^{d-1} x^{2^i}$. Compute $\gcd(r, f \circ t)$ for random choices of $t \in \mathbb{Z}_2[x]$ of degree less than d.

7.9.1. Example. We demonstrate this algorithm via an explicit example. Consider the polynomial $q(x)$ in $\mathbb{Z}_5[x]$ given by

$$q(x) = x^{19} + 3x^{18} + x^{17} + x^{16} - x^{15} + x^{14} + x^{12} + x^{11} - 2x^{10} + x^9 - 2x^8 - 2x^6 + 2x^5 + x^4 - x^3 + 2x^2 + 2x - 2.$$

First a computation shows that $\gcd(q, q') = 1$. Then we compute

$$\gcd(q, x^5 - x) = x^2 + 3x + 2 = (x + 1)(x + 2).$$

Factoring this out leaves $q_1 = q/(x^2 + 3x + 2)$. Continue

$$\gcd(q_1, x^{25} - x) = 1$$

showing that there are no quadratic factors. Then

$$\gcd(q_1, x^{125} - x) = x^9 + 2x^7 - x^6 - 2x^4 - x^3 + x^2 + 1.$$

This must be the product of three irreducible polynomials of degree 3. Since $\frac{5^3-1}{2} = 62$, we compute

$$\gcd(x^9 + 2x^7 - x^6 - 2x^4 - x^3 + x^2 + 1, x^{62} - 1) = x^3 + 2x - 1.$$

So

$$x^9 + 2x^7 - x^6 - 2x^4 - x^3 + x^2 + 1 = (x^3 + 2x - 1)(x^6 - 2x - 1).$$

And

$$\gcd(x^6 - 2x - 1, (x + 1)^{62} - 1) = x^3 - x^2 - 2.$$

Hence

$$x^9 + 2x^7 - x^6 - 2x^4 - x^3 + x^2 + 1 = (x^3 + 2x - 1)(x^3 - x^2 - 2)(x^3 + x^2 + x - 2).$$

The remaining term is

$$\begin{aligned} q_3 &= q_1/(x^9 + 2x^7 - x^6 - 2x^4 - x^3 + x^2 + 1) \\ &= x^8 + 2x^6 - 1 \end{aligned}$$

This is either irreducible, or the product of two irreducible factors of degree 4. We try

$$\gcd(q_3, x^{625} - x) = q_2$$

So q_2 is a product of quartics

$$\begin{aligned} \gcd(q_3, x^{312} - 1) &= 1 \\ \gcd(q_3, (x + 1)^{312} - 1) &= x^4 + x^2 - 2x + 2 \end{aligned}$$

Thus

$$x^8 + 2x^6 - 1 = (x^4 + x^2 - 2x + 2)(x^4 + x^2 + 2x + 2).$$

This provides a complete factorization of $q(x) =:$

$$(x + 1)(x + 2)(x^3 + 2x - 1)(x^3 - x^2 - 2)(x^3 + x^2 + x - 2) \times (x^4 + x^2 - 2x + 2)(x^4 + x^2 + 2x + 2).$$

Exercises

1. Use the distinct degree algorithm to factor $q \in \mathbb{Z}_7[x]$ given by
$x^{12} + 3x^{11} + 3x^{10} + x^9 + 2x^8 + +6x^6 + 6x^5 + x^4 + 3x^3 + x^2 + 4x + 3.$

2. Use the distinct degree algorithm to factor the polynomial $q \in \mathbb{Z}_5[x]$ given by

$$q(x) = x^8 + x^7 + 3x^6 + 2x^5 + 4x^4 + 4x^3 + 3x + 4.$$

3. Factor in $\mathbb{Z}_3[x]$:

$$q(x) = x^{16} + x^{14} + x^{12} - x^8 - x^6 + x^2 + 1.$$

4. Let $f(x) = \sum_{i=1}^{d-1} x^{2^i} \in \mathbb{Z}_2[x]$. Show that $f(f(x) + 1) = x^{2^d} - 1$.

5. Factor in $\mathbb{Z}_2[x]$ the polynomial $q(x) =$
$x^{17} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x + 1.$

Remember to check for repeated factors.

7.10. Factoring Rational Polynomials

Now let us reconsider the problem of factoring polynomials with integer coefficients. This can now be done in a routine algorithmic way. The first step is to pick a prime p relatively prime to the leading coefficient of the polynomial q. For a computer, a good choice is reasonably large but still manageable for exact integer arithmetic. (MAPLE picks one near 10^4.) Then use the distinct degree algorithm to factor $q(x) \pmod p$. Finally, use an algorithm we explain in this section known as Hensel's Lemma to recursively improve this factorization mod p to a factorization mod p^k until p^k is large enough to bound the coefficients of the factors. This either yields a factorization or shows that one does not exist.

This kind of search can be carried out efficiently on a computer. Moreover, it is not very difficult to get crude bounds on the size of the coefficients of possible factors. For example, if $q = \sum_{i=0}^{d} q_i x^i$ is a factor of $p = \sum_{i=0}^{n} p_i x^i$, then

$$\sum_{i=0}^{d} |q_i| \le 2^d \Big(\sum_{i=0}^{n} |p_i|^2 \Big)^{1/2}.$$

We will not prove such an estimate here. However, it means that normally only a few applications of Hensel's Lemma will do the job. Once k is sufficiently large, we either find an integer factorization or realize that none exists.

We make two simplifying assumptions that are easily achieved. Choose the prime p so that it is relatively prime to the leading coefficient of our given polynomial $q \in \mathbb{Z}[x]$. Also, assume that q factors in $\mathbb{Z}_p[x]$ into a product uv where u and v are relatively prime. Of course, if q is irreducible in $\mathbb{Z}_p[x]$,

then q is irreducible in $\mathbb{Z}[x]$ by Corollary 6.5.2 and thus in $\mathbb{Q}[x]$ by Gauss's Lemma 6.3.3.

7.10.1 Hensel's Lemma. *Suppose that* $q(x) = \sum_{i=0}^{d} q_i x^i$ *factors as* $q \equiv uv \pmod{p}$. *Furthermore, assume that* $\gcd(q_d, p) = 1$ *and that* u *and* v *are relatively prime in* $\mathbb{Z}_p[x]$. *Then there is an algorithm to calculate polynomials* u_k *and* v_k *in* $\mathbb{Z}[x]$ *so that*

$$q \equiv u_k v_k \pmod{p^k}$$

with $\deg(u_k) = \deg(u)$ *and* $\deg(v_k) = \deg(v)$.

Proof. When the leading coefficient of q isn't 1, there is a slight problem because the leading coefficients of the factors u and v aren't determined. However, they must be divisors of q_d. So a simple trick deals with this problem. Replace $q(x)$ by $q_d q(x)$ and multiply u and v by the appropriate factor so that their leading coefficient is also q_d. Since the identity $q \equiv uv$ is only mod p, this adjustment can be made mod p, and then fixed up in the integers by adding some multiple of px^m.

We will also assume that $m = \deg(u) \leq deg(v) = n$. By hypothesis, $\gcd(u, v) = 1$ in $\mathbb{Z}_p[x]$. Thus by the Euclidean algorithm there are polynomials s and t in $\mathbb{Z}[x]$ so that

$$su + tv \equiv 1 \pmod{p}.$$

Let $u_1 = u$ and $v_1 = v$ and define $r_1 = (q - u_1 v_1)/p$ which has integer coefficients by hypothesis. In fact, we only need $r_1 \pmod{p}$. Now find integer polynomials s_1 and t_1 so that

$$s_1 u_1 + t_1 v_1 \equiv r_1 \pmod{p}$$

such that $\deg(s_1) < n$ and $\deg(t_1) < m$. To obtain this, notice that

$$(r_1 s)u_1 + (r_1 t)v_1 \equiv r_1(su + tv) \equiv r_1 \pmod{p}.$$

Divide u_1 into $r_1 t$ to obtain quotient a_1 and remainder t_1 with $\deg(t_1) < m$. Set $s_1 = r_1 s + a_1 v_1 \pmod{p}$. We see that (s_1, t_1) is a solution with control on $\deg(t_1)$. The point is that $t_1 v_1$ is a polynomial of degree

$$\deg(t_1) + \deg(v_1) < m + n.$$

By the identity $s_1 u_1 \equiv 1 - r_1 v_1 \pmod{p}$, we see that the same is true for $s_1 u_1$. Since s_1 was reduced mod p, we know that it has a leading coefficient relatively prime to p. Thus its degree is the same as its degree mod p. So,

$$\deg(s_1) = \deg(s_1 u_1) - \deg(u_1) < m + n - m = n.$$

Now we are ready to improve the factorization. Set

$$u_2 := u_1 + pt_1 \qquad v_2 := v_1 + ps_1.$$

This does not affect the leading coefficients of the u's or v's. Then it is a simple exercise to verify

$$\begin{aligned} q - u_2v_2 &= (u_1v_1 + pr_1) - (u_1v_1 + p(s_1u_1 + t_1v_1) + p^2s_1t_1) \\ &= p(r_1 - s_1u_1 - t_1v_1) + p^2s_1t_1 \equiv 0 \pmod{p^2}. \end{aligned}$$

This procedure repeats recursively. Indeed, if

$$q \equiv u_kv_k \pmod{p^k},$$

define $r_k = (q - u_kv_k)/p^k$. As above, set t_k to be the remainder on dividing r_kt by u_k with quotient a_k. Then set $s_k = r_ks + a_kv_k \pmod{p}$. The new approximation is given by

$$u_{k+1} := u_k + p^kt_k \qquad v_{k+1} := v_k + p^ks_k.$$

Then

$$\begin{aligned} q - u_{k+1}v_{k+1} &= (u_kv_k + p^kr_k) - \big(u_kv_k + p^k(s_ku_k + t_kv_k) + p^{2k}s_kt_k\big) \\ &= p^k(r_k - s_ku_k - t_kv_k) + p^{2k}s_kt_k \equiv 0 \pmod{p^{k+1}}. \end{aligned}$$

Since this is accurate modulo p^{k+1}, reduce the coefficients mod p^{k+1} symmetrically about 0 so that the coefficients have modulus at most $p^{k+1}/2$.

Repeating this procedure increases the 'accuracy' of the factorization by a factor of p at each stage. Moreover, every stage is a routine calculation. The most complicated step, the Euclidean algorithm, is executed only once. On a computer, this procedure is very efficient. ■

7.10.2. Example. Let us work through an example. The calculations were done by a computer, although with such a small example, it is almost practical to do it by hand. Let

$$q(x) = 6x^7 + 53x^6 - 174x^5 + 300x^4 - 33x^3 - 293x^2 + 453x - 81.$$

Suppose that we found the factorization

$$q \equiv (x^3 + 2x^2 + 2x + 2)(x^4 + x^3 + 2x^2 + 2x + 2) \pmod{5}.$$

Following our algorithm, we replace q by $Q = 6q \pmod{5}$, and set

$$\begin{aligned} u_1 = 6u &\equiv 6x^3 + 2x^2 + 2x + 2 \pmod{5} \\ v_1 = 6v &\equiv 6x^4 + 1x^3 + 2x^2 + 2x + 2 \pmod{5} \end{aligned}$$

By the Euclidean algorithm, solve $su_1 + tv_1 \equiv 1 \pmod{5}$:

$$s = -x^3 - x^2 + 3 \qquad t = x^2 + 2x.$$

The first step is to compute the remainder

$$\begin{aligned} r_1 &= (Q - u_1v_1)/5 \\ &= 42x^6 - 252x^5 + 288x^4 - 126x^3 - 438x^2 + 486x - 126 \\ &\equiv 2x^6 + 3x^5 + 3x^4 + 4x^3 + 2x^2 + x + 4 \pmod{5} \end{aligned}$$

Then dividing tr_1 by u_1 mod 5 yields remainder $t_1 = x + 2$ and quotient a_1 which is used to compute

$$s_1 = sr_1 + a_1 v_1 \equiv 2x^3 + 3x^2 \pmod 5.$$

Then we obtain

$$\begin{array}{rcrcrl} u_2 & \equiv & u_1 + 5t_1 & \equiv & 6x^3 + 12x^2 - 8x - 3 & \pmod{25} \\ v_2 & \equiv & v_1 + 5s_1 & \equiv & 6x^4 - 9x^3 + 2x^2 + 12x + 12 & \pmod{25} \end{array}$$

Check the remainder

$$r_2 = (Q - u_2 v_2)/25 \equiv 2x^6 + 4x^5 + x^4 + 3x^3 + 3x^2 + 4x + 2 \pmod 5.$$

This isn't 0, so continue on. We get $t_2 = 4x^2 + x$ is the remainder of tr_2 on dividing by u_2 mod 5 to get quotient a_2. And

$$s_2 \equiv sr_2 + a_2 v_2 \equiv 3x^2 + 3x + 1 \pmod 5.$$

Then the next approximants are

$$\begin{array}{rcrcrl} u_3 & \equiv & u_2 + 25t_2 & \equiv & 6x^3 - 13x^2 + 17x - 3 & \pmod{125} \\ v_3 & \equiv & v_2 + 25s_2 & \equiv & 6x^4 - 59x^3 - 48x^2 + 12x + 37 & \pmod{125} \end{array}$$

This time the remainder is

$$r_3 = (Q - u_3 v_3)/125 \equiv x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 2 \pmod 5.$$

This still isn't 0, so continue on. We get $t_3 = 0$ is the remainder of tr_3 on dividing by u_3 mod 5 to get quotient a_3. And

$$s_3 \equiv sr_3 + a_3 v_3 \equiv x^3 + 1 \pmod 5.$$

Then the next approximants are

$$\begin{array}{rcrcrl} u_4 & \equiv & u_3 + 125t_3 & \equiv & 6x^3 - 13x^2 + 17x - 3 & \pmod{625} \\ v_4 & \equiv & v_3 + 125s_3 & \equiv & 6x^4 + 66x^3 - 48x^2 + 12x + 162 & \pmod{625} \end{array}$$

This time we have found the factorization

$$Q = (6x^3 - 13x^2 + 17x - 3)(6x^4 + 66x^3 - 48x^2 + 12x + 162)$$

whence

$$q = (6x^3 - 13x^2 + 17x - 3)(x^4 + 11x^3 - 8x^2 + 2x + 27).$$

Exercises

1. Using computer software, follow the above procedure with $p = 7$ to factor

$$q(x) = 6x^7 + 43x^6 - 363x^5 - 301x^4 + 527x^3 - 15x^2 - 387x + 76.$$

2. Factor in $\mathbb{Z}[x]$ the polynomial $q(x) = x^{14} + 31x^{13} - 2x^{11} - 63x^{10} + 31x^9 + 27x^8 + 897x^7 + 33x^6 + 4x^5 + 54x^4 + 3x^3 - 58x^2 + 27x + 1$ given that

$$q(x) \equiv (x^7 + x^6 + 2x^3 + 3x + 1)(x^7 + 3x^4 + x^3 - x + 1) \pmod 5.$$

Notes on Chapter 7

It was Galois who first realized that $\mathbb{Z}_p[x]/(q)$ formed a field for any irreducible polynomial q. He introduced the idea of *adjoining* a root of a polynomial to build a larger field. Dedekind was the first to suggest that there should be a general definition of field, although for him, a field was always a subset of $\mathbb{C}$. This was the beginning of a deeper understanding of the relationship between algebra and number theory. Kronecker's work was very influential: he allowed for a more abstract extension of a field by roots of polynomials. E.H. Moore classified finite fields in 1893.

Dedekind and Weber constructed certain fields of analytic functions associated to Riemann surfaces, and Hensel constructed the field of p-adic numbers. These very different types of fields paved the way to a general abstract definition of fields due to Steinitz in 1910. Many general theorems in field theory and Galois theory were proven by Weber and Steinitz. Subsequent work of Emil Artin modernized the treatment of Galois theory.

See Kleiner's short monograph [**19**] for a brief history of modern algebra. Emil Artin's book [**4**] on Galois theory is a nice introduction to field theory. See Lidl and Niederreiter [**24**] for more detailed information about finite fields. Michael Artin's comprehensive book on algebra [**5**] covers field theory including a chapter on quadratic number fields.

The discovery of algorithms for the factorization of polynomials is more recent. See Knuth [**21**, Section 4.6.2] for an overview of various methods. Berlekamp [**6**] found the first general algorithm for factoring polynomials in $\mathbb{Z}_p[x]$ by reducing the problem to a large system of linear equations. The method discussed in these notes is due to D. Cantor and H. Zassenhaus [**7**] in 1981. Hensel's lemma dates back to 1904 in the same paper in which he introduced p-adic number fields.

Bibliography

[1] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793, DOI 10.4007/annals.2004.160.781. MR2123939

[2] Ş. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press, Cambridge, 2004. MR2031707

[3] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722, DOI 10.2307/2118576. MR1283874

[4] E. Artin, *Galois theory*, 2nd ed., Dover Publications, Inc., Mineola, NY, 1998. Edited and with a supplemental chapter by Arthur N. Milgram. MR1616156

[5] M. Artin, *Algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[6] E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell System Tech. J. **46** (1967), 1853–1859, DOI 10.1002/j.1538-7305.1967.tb03174.x. MR219231

[7] D. G. Cantor and H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981), no. 154, 587–592, DOI 10.2307/2007663. MR606517

[8] R. L. Cooke, *The history of mathematics: A brief course*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2013. MR3236642

[9] L. E. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality. Vol. II: Diophantine analysis. Vol. III: Quadratic and higher forms.*, Chelsea Publishing Co., New York, 1966.

[10] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **IT-22** (1976), no. 6, 644–654, DOI 10.1109/tit.1976.1055638. MR437208

[11] P. Erdös, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206, DOI 10.5486/pmd.1956.4.3-4.16. MR79031

[12] D. J. H. Garling, *A course in mathematical analysis. Vol. I: Foundations and elementary real analysis*, Cambridge University Press, Cambridge, 2013, DOI 10.1017/CBO9781139424493. MR3087523

[13] W. J. Gilbert and S. A. Vanstone, *An introduction to mathematical thinking: Algebra and number systems*, Pearson Prentice Hall, Upper Saddle River, NJ, 2005. MR2128503

[14] J. Gray, *A history of abstract algebra: From algebraic equations to modern algebra*, Springer Undergraduate Mathematics Series, Springer, Cham, 2018, DOI 10.1007/978-3-319-94773-0. MR3823206

[15] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman; With a foreword by Andrew Wiles. MR2445243

[16] R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J. **29** (1950), 147–160, DOI 10.1002/j.1538-7305.1950.tb00463.x. MR35935
[17] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38, DOI 10.1093/qmath/37.1.27. MR830627
[18] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220, DOI 10.1515/crll.1967.225.209. MR207630
[19] I. Kleiner, *A history of abstract algebra*, Birkhäuser Boston, Inc., Boston, MA, 2007, DOI 10.1007/978-0-8176-4685-1. MR2347309
[20] I. Kleiner, *Excursions in the history of mathematics*, Birkhäuser/Springer, New York, 2012, DOI 10.1007/978-0-8176-8268-2. MR3222782
[21] D. E. Knuth, *The art of computer programming. Vol. 2: Seminumerical algorithms*, Addison-Wesley, Reading, MA, 1998. Third edition [of MR0286318]. MR3077153
[22] R. Laubenbacher and D. Pengelley, *"Voici ce que j'ai trouvé:" Sophie Germain's grand plan to prove Fermat's last theorem* (English, with English and French summaries), Historia Math. **37** (2010), no. 4, 641–692, DOI 10.1016/j.hm.2009.12.002. MR2735899
[23] H. W. Lenstra Jr. and C. Pomerance, *Primality testing with Gaussian periods*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 4, 1229–1269, DOI 10.4171/JEMS/861. MR3941463
[24] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986. MR860948
[25] J. H. Manheim, *The genesis of point set topology*, Pergamon Press, Oxford-Paris-Frankfurt; The Macmillan Company, New York, 1964. MR0226976
[26] G. L. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13** (1976), no. 3, 300–317, DOI 10.1016/S0022-0000(76)80043-8. MR480295
[27] M. Ram Murty, *Prime numbers and irreducible polynomials*, Amer. Math. Monthly **109** (2002), no. 5, 452–458, DOI 10.2307/2695645. MR1901498
[28] Q. I. Rahman and G. Schmeisser, *Analytic theory of polynomials*, London Mathematical Society Monographs. New Series, vol. 26, The Clarendon Press, Oxford University Press, Oxford, 2002. MR1954841
[29] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138, DOI 10.1016/0022-314X(80)90084-0. MR566880
[30] P. Ribenboim, *Fermat's last theorem for amateurs*, Springer-Verlag, New York, 1999. MR1719329
[31] P. Ribenboim, *The little book of bigger primes*, 2nd ed., Springer-Verlag, New York, 2004. MR2028675
[32] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), no. 2, 120–126, DOI 10.1145/359340.359342. MR700103
[33] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 124–134, DOI 10.1109/SFCS.1994.365700. MR1489242
[34] J. H. Silverman, *A Friendly Introduction to Number Theory*, 4th ed., Pearson Education, Inc., Upper Saddle River, NJ, 2012.
[35] B. Simon, *Basic complex analysis*, A Comprehensive Course in Analysis, Part 2A, American Mathematical Society, Providence, RI, 2015, DOI 10.1090/simon/002.1. MR3443339
[36] S. Singh, *The code book: The Secret History of Codes and Code Breaking*, Fourth Estate and Doubleday, 1999.
[37] H. M. Stark, *An introduction to number theory*, MIT Press, Cambridge, Mass.-London, 1978. MR514402
[38] J. V. Uspensky, *Theory of equations*, McGraw-Hill Book Co., New York, 1948.

Index

Published Titles in This Series

31 **Kenneth R. Davidson and Matthew Satriano,** Integer and Polynomial Algebra, 2023
30 **Jonathan K. Hodge and Richard E. Klima,** The Mathematics of Voting and Elections: A Hands-On Approach, Second Edition, 2018
29 **Margaret Cozzens and Steven J. Miller,** The Mathematics of Encryption, 2013
28 **David Wright,** Mathematics and Music, 2009
27 **Jacques Sesiano,** An Introduction to the History of Algebra, 2009
26 **A. V. Akopyan and A. A. Zaslavsky,** Geometry of Conics, 2007
25 **Anne L. Young,** Mathematical Ciphers, 2006
24 **Burkard Polster,** The Shoelace Book, 2006
23 **Koji Shiga and Toshikazu Sunada,** A Mathematical Gift, III, 2005
22 **Jonathan K. Hodge and Richard E. Klima,** The Mathematics of Voting and Elections: A Hands-On Approach, 2005
21 **Gilles Godefroy,** The Adventure of Numbers, 2004
20 **Kenji Ueno, Koji Shiga, and Shigeyuki Morita,** A Mathematical Gift, II, 2004
19 **Kenji Ueno, Koji Shiga, and Shigeyuki Morita,** A Mathematical Gift, I, 2003
18 **Timothy G. Feeman,** Portraits of the Earth, 2002
17 **Serge Tabachnikov, Editor,** Kvant Selecta: Combinatorics, I, 2002
16 **V. V. Prasolov,** Essays on Numbers and Figures, 2000
15 **Serge Tabachnikov, Editor,** Kvant Selecta: Algebra and Analysis, II, 1999
14 **Serge Tabachnikov, Editor,** Kvant Selecta: Algebra and Analysis, I, 1999
13 **Saul Stahl,** A Gentle Introduction to Game Theory, 1999
12 **V. S. Varadarajan,** Algebra in Ancient and Modern Times, 1998
11 **Kunihiko Kodaira, Editor,** Basic Analysis: Japanese Grade 11, 1996
10 **Kunihiko Kodaira, Editor,** Algebra and Geometry: Japanese Grade 11, 1996
9 **Kunihiko Kodaira, Editor,** Mathematics 2: Japanese Grade 11, 1997
8 **Kunihiko Kodaira, Editor,** Mathematics 1: Japanese Grade 10, 1996
7 **Dmitri Fomin, Sergey Genkin, and Ilia V. Itenberg,** Mathematical Circles, 1996
6 **David W. Farmer and Theodore B. Stanford,** Knots and Surfaces, 1996
5 **David W. Farmer,** Groups and Symmetry: A Guide to Discovering Mathematics, 1996
4 **V. V. Prasolov,** Intuitive Topology, 1994
3 **L. E. Sadovskiĭ and A. L. Sadovskiĭ,** Mathematics and Sports, 1993
2 **Yu. A. Shashkin,** Fixed Points, 1991
1 **V.M. Tikhomirov,** Stories about Maxima and Minima, 1991

This book is a concrete introduction to abstract algebra and number theory. Starting from the basics, it develops the rich parallels between the integers and polynomials, covering topics such as Unique Factorization, arithmetic over quadratic number fields, the RSA encryption scheme, and finite fields.

In addition to introducing students to the rigorous foundations of mathematical proofs, the authors cover several specialized topics, giving proofs of the Fundamental Theorem of Algebra, the transcendentality of e, and Quadratic Reciprocity Law. The book is aimed at incoming undergraduate students with a strong passion for mathematics.

ISBN 978-1-4704-7332-7

9 781470 473327

MAWRLD/31

For additional information and updates on this book, visit

www.ams.org/bookpages/mawrld-31

AMS
www.ams.org